SP/02 to SWIM TF/11

API Management and Gateway Introduction, Framework and Best Practices (for Req-Reply Messaging)

SWIM Task Force 11

May 25-29, 2026

Presented By:
FAA SWIM Program Office

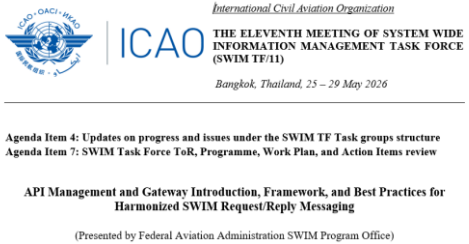
Federal Aviation Administration

Introduction

With emerging web technologies and applications to future of flight planning and data sharing, the Federal Aviation Administration (FAA) and Asia-Pacific (APAC) region are considering Application Programming Interface (API) Management and Gateway solutions for Request-Reply SWIM data message exchange—in addition to using event brokers for asynchronous (pub-sub) messaging for comprehensive messaging aveneues in alignment with industry best practices.

System Wide Information Management (SWIM) provides a single point of access for near real-time aeronautical, flight, weather, and surveillance information and serves as the **digital backbone for the future of flight data sharing and air traffic management.**

API Gateways and Management solutions enable scalable, secure, and reliable digital services through **centralized routing, security, monitoring, governance, access control, and lifecycle management.**



International Civil Aviation Organization

ICAO

THE ELEVENTH MEETING OF SYSTEM WIDE INFORMATION MANAGEMENT TASK FORCE (SWIM TF/11)

Bangkok, Thailand, 25 – 29 May 2026

Agenda Item 4: Updates on progress and issues under the SWIM TF Task groups structure
Agenda Item 7: SWIM Task Force ToR, Programme, Work Plan, and Action Items review

API Management and Gateway Introduction, Framework, and Best Practices for Harmonized SWIM Request/Reply Messaging

(Presented by Federal Aviation Administration SWIM Program Office)

The working paper provides an overview of the latest FAA and APAC developments on API Gateways for SWIM messaging, benefits of an API Gateway and Management solution, **best practices to develop a framework on API governance and harmonized cross-regional SWIM data exchange.**

FAA and APAC Collaboration

- **Federal Aviation Administration (FAA), Korea Airports Corporation (KAC), and Civil Aviation Authority of Singapore are working under the SWIM Implementation Pioneer Group (SIPG) and APAC SWIM TF initiatives to develop harmonized, interoperable SWIM messaging aligned with International Civil Aviation Organization (ICAO) standards.**

- **SIPG Task 3 is leading APAC Request-Reply MEP implementation efforts on the following in coordination with relevant ICAO APAC groups (ex: FF-ICE ad-hoc):**
  - Request-Reply Message Exchange Patterns (MEP) Guidance documentation
  - RESTful API Naming and Structuring Guidance Material documentation
  - API Gateway Requirements Specification document in APAC Region
  - Prototype implementation and testing Request-Reply MEP (both sync. and async.)

- FAA is modernizing SWIM infrastructure through API Management and Gateway solutions to support future flight planning web services and event-driven messaging architectures. **The FAA is modernizing its SWIM messaging infrastructure with API Gateways for synchronous messaging and Event-Brokers for asynchronous messaging.**

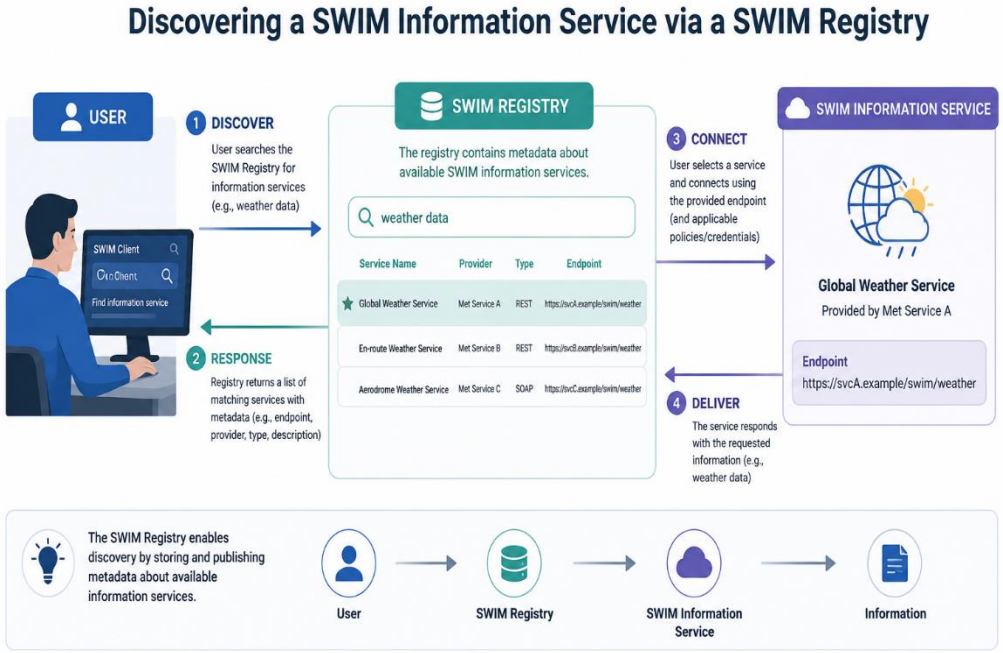
Digital Modernization with AMHS- SWIM Transition

- The aviation industry is **transitioning from AFTN/AMHS message-switching networks** and standardized addressing/delivery headers **to SWIM's service-oriented architecture, where users discover services/endpoints through registries and invoke them directly through standardized interfaces**

- **In a properly designed SWIM environment, routing is inherent in the service invocation itself,** the consumer knows which service it needs, discovers where that service is, and calls it.

- **Challenge for global SWIM implementation is not to replicate AFTN's message-switching model with new metadata headers, but to ensure that information services are well-described, discoverable, and accessible across organizational and regional boundaries.**

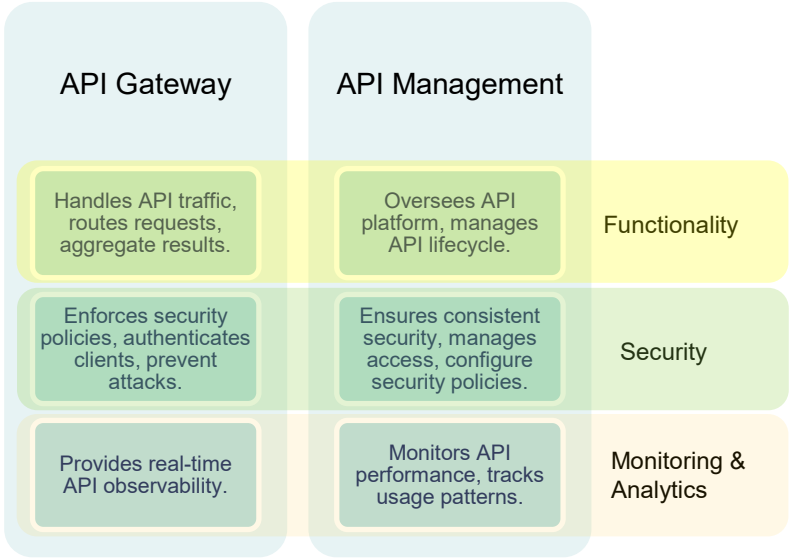
- **The ICAO Information Service Definition (ISD) framework and SWIM registry interoperability work already underway are the primary vehicles for achieving this.**



API Gateways and Management platforms, as described in this paper, provide one proven implementation approach for centralize access management, discovery, protocol mediation, and traffic governance for their SWIM services

API Gateway and API Management

- APIs enable standardized communication and cross-border data sharing between aviation stakeholders, improving collaborative decision-making and real-time operational coordination.
- API Gateways provide centralized security and traffic management, including authentication, authorization, encryption, protocol mediation, and prioritization of critical aviation services.
- API Management platforms support governance and lifecycle management through monitoring, analytics, developer portals, service publication, and SLA oversight.



API Management Enterprise Benefits

Simplified API Design: Create web APIs of all types (REST, SOAP, gRPC, GraphQL, Webhooks etc.); and Full API lifecycle management.

Comprehensive management and security: Centrally integrated IAM, advanced security, governance, automated workflows, testing, traffic management.

Telco and Environment agnostic solution: Can be deployed in any environment independent of the network infrastructure. Harmonized SWIM modernization on-prem and in cloud.

Monitoring & SLA Tracking: Built-in monitoring/logging, SLA tracking. Native integration with enterprise monitoring tool, Datadog, for 1st and 2nd level support.

Unified Management and Developer Portal: Discovery and access to all NAS information services from a common interface. Native federation with COTS Messaging Platforms across the NAS portfolio (Solace, Google/Apigee, AWS etc).

Integration with Event-Brokers. Protocol mediation to expose async events as web services (ex: JMS/AMQP to REST) or federation for discovery.

Cost savings and Enterprise inheritance: Prevents duplicative costs and conflicting governance, security, and implementation from standalone solutions. Inherit cross cutting enterprise controls to simplify system design.

Decouples Service Providers and consumers: Introduce an abstraction layer between consumer facing interfaces and backend implementations

Discussions – API Gateway and Management

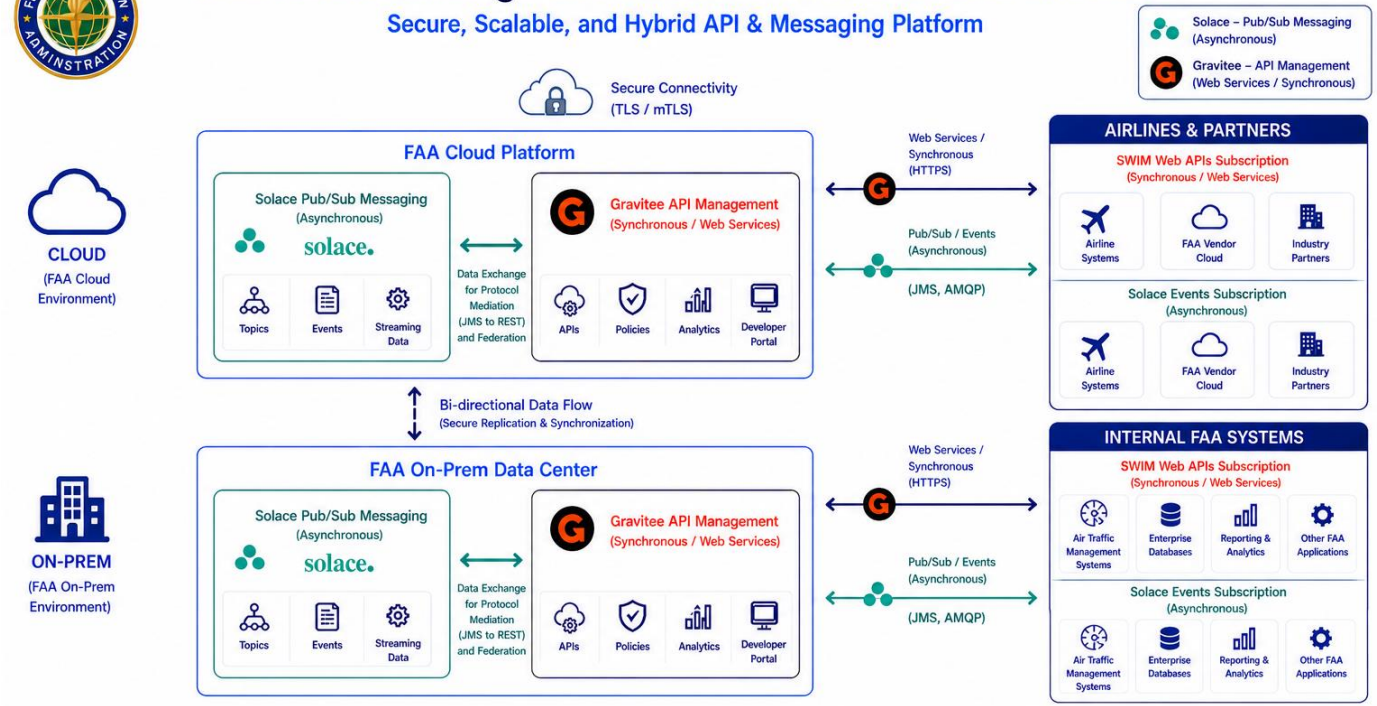
- It is critical to establish both an API Manager and Gateway when implementing cross regional API data exchange.
  - API gateways alone handle runtime functions like routing, traffic control, and basic security, but they do not provide full lifecycle management.
  - API manager complements gateways by offering centralized capabilities such as policy governance, analytics, developer onboarding, documentation, and version control.
- Together, they ensure APIs are not only efficiently routed and secured in real time, but also consistently designed, monitored, and maintained over time.
- This combination improves visibility, enforces standards, simplifies administration, and enables organizations to scale their API ecosystem in a controlled and strategic way.

Key Benefits

- **Centralized API platform** for routing, governance, and service management
- **Enhanced security** through authentication, authorization, mTLS, IAM, and rate limiting
- **Access control & Zero Trust support** with secure credential management
- **Improved performance** using caching, load balancing, and traffic optimization
- **Network & infrastructure agnostic** for cloud, VPN, hybrid, or on-prem deployments
- **Multi-protocol support** including REST, SOAP, gRPC, GraphQL, streaming, and event-driven APIs (ex: JMS/AMQP to REST)
- **Protocol mediation & interoperability** between modern and legacy systems
- **Centralized API registration & publishing** for service discovery and management
- **Schema validation** to ensure compliant and properly structured API messages
- **Real-time API monitoring & analytics** for traffic visibility, SLA tracking, and auditing
- **API version management** supporting upgrades, deprecation, and consumer migration
- **Reduced backend complexity** by offloading governance and security functions to APIM

FAA Data Exchange Architecture with Solace & Gravitee

Secure, Scalable, and Hybrid API & Messaging Platform



- **Solace and Gravitee power FAA's Event broker and API Manageement and Gateway solution .**
- Event-brokers and API Gateways solve different problems (both are vital but serve different use cases).
- API gateways are best geared to handle synchronous request/response interactions where a client needs an immediate answer (ex: submitting and acknowledging a flight plan, expose filing service).
- Event brokers handle asynchronous events distribution between loosely coupled services, where direct response isn't required.
- Event-brokers and API Gateways integrated together offer a comprehensive and unified data management platform for SIWM messaging.

FOUNDATIONAL CAPABILITIES

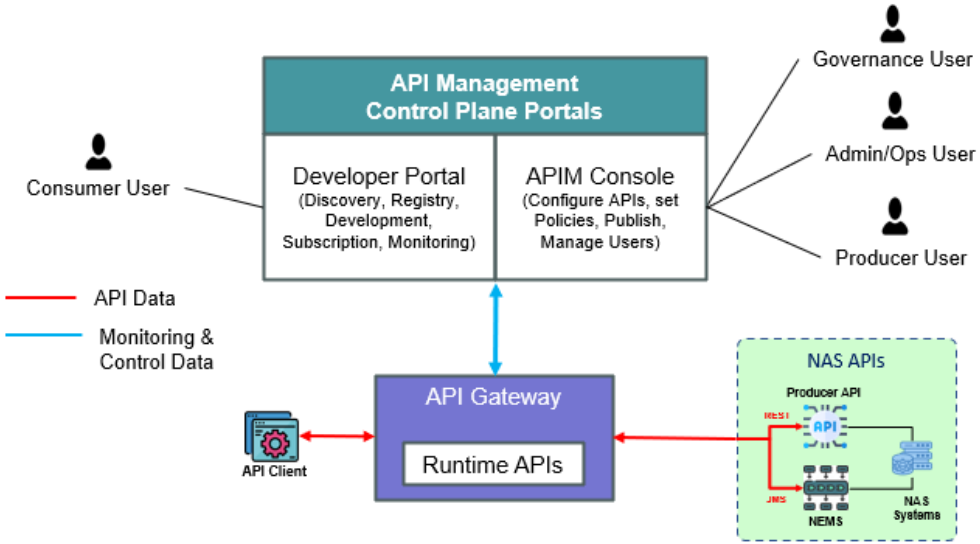
- Security (TLS/mTLS, OAuth2, RBAC)
- Governance & Policy Enforcement
- Monitoring & Observability (Logs, Metrics, Traces)
- High Availability & Scalability
- Hybrid (Cloud & On-Prem) Flexibility
- Developer Experience (Self-Service)

KEY ARCHITECTURE PRINCIPLES

- Airlines & Partners, External FAA Vendor Managed Clouds, and Internal FAA Systems consume data via Gravitee (synchronous) and Solace (asynchronous).
- Airlines & Partners exchange data only with the FAA Cloud Platform.
- On-Prem platform replicated with Cloud for resilience and consistency.
- Internal FAA Systems consume data from On-Prem via asynchronous messaging (JMS).

Simplified FAA API Management Architecture

- APIs, API gateways, and API management platforms work together to enable secure, controlled access to backend systems
- SWIM exposes producer APIs, which are accessed through an API Gateway
- API Management Control Plane, which provides governance and lifecycle management through two main portals:
  - **Developer Portal** for discovery, registry access
  - **Admin Console** for control plane, gateway configurationm and management



API User Types

API User	Activity
API Producer	**Design, document, and maintain APIs**. Register or publish APIs in the catalog, configure gateway policies, and manage API lifecycle from development through retirement.
API Consumer	**Discover, subscribe and integrate APIs** into applications. **Register applications**, manage credentials and comply with usage quotas and security requirements.
Governance	Responsible for **defining, enforcing, and maintaining standards, policies, and best practices across the API lifecycle.** Their role focuses on ensuring consistency, compliance, and quality by establishing guidelines for API design, security, versioning, and documentation. Governance users also review and approve APIs, monitor adherence to organizational and regulatory requirements.
Administrator & Operations	Responsible for **configuring and overseeing the overall platform and its environment. This includes managing user access and roles, setting up API gateways, and maintaining system configurations.** Admin users ensure the platform operates smoothly by handling tasks like onboarding users, monitoring system health, and troubleshooting issues. They also support governance and security efforts by enforcing access controls and ensuring the API management infrastructure is properly maintained.
Cybersecurity	**Ensures compliance with security policies, IAM, and Zero Trust principles.** Define and enforce authentication, authorization, and data protection requirements (ex: mTLS).

Recommended framework for API Governance and Best Practices

Best Practice	Description
Service description and Nomenclature	▪ Leverage standard naming conventions (ex: URI) for consistent documentation and simplified lifecycle management ▪ Leverage industry standard templates such as OpenAPI specifications to leverage universally established machine-readable formats to describe web services
API Versioning	▪ Leverage structured mechanisms for managing evolution of APIs. ▪ Manage multiple versions of the same API and facilitate consumer management and migration ▪ Identify versioning strategy such as URI path versioning, Header Versioning, semantic versioning,
API Registry	▪ All APIs shall be registered and published to the API registry for user discovery ▪ Developers shall also provide detailed documentation such as API specifications, schema definitions, access controls, use limitations, error handling guidance etc.
Authentication and Authorization	▪ All SWIM APIs shall be enforced with certificate based authentication and leverage mutual TLS for end to end encrypted data exchange ▪ All APIs shall include policy enforcement such as OAuth 2.0, JWT ▪ All APIs shall be integrated with Identity Access Management solutions for Role Based Access Control and Certificate management ▪ Leverage API keys or secrets to manage API access and credentials

Recommended framework for API Governance and Best Practices cont'd.

Best Practice	Description
Schema Validation	▪ API Gateways shall perform XML schema validation to ensure message payload satisfies expected data structure and that any malformed and non-compliant messages are rejected
Traffic Management	▪ Implement rate limits and throttling at Gateway level to manage incoming traffic requests per minute and minimize system overload
Decoupled services	▪ Establish API proxies to isolate external APIs from backend APIs and enable users to simply discover and consume from API endpoint without requiring knowledge of underlying infrastructure
SLAs	▪ Establish Service Level Agreements as appropriate for service uptime
API contracts	▪ Implement API contracts to establish how an API provider and consumer application will interact with each other (ex: endpoint, HTTP method, authentication)

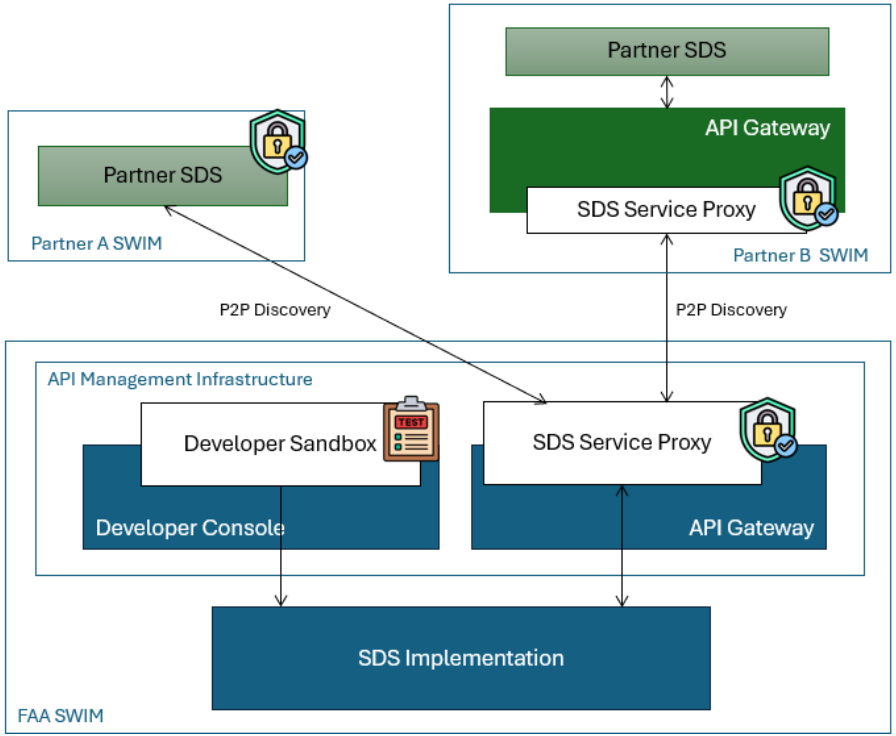
Use Case – SWIM Discovery Services (SDS)

- **The FAA will be implementing SDS via an API Gateway that enforces OAuth 2.0 and mutual TLS** for secure and harmonized connection with international registries.

- **SDS will be integrated with an API Management (APIM) capability to enhance the design-time** and runtime capabilities **and governance for FAA's SWIM implementation.**

- **APIM will enable SDS with security, rate limiting, schema validation, throttling, caching, and message transformation.**

- APIM will also provide robust API management and governance capabilities, such as policy enforcement, developer onboarding, as well as monitoring and analytics.



Use Case – FF-ICE

Flight and Flow Information for a Collaborative Environment (FF-ICE) demonstrates APIM's capabilities in modernizing international flight planning through collaborative information exchange.

1. **Discovery & Subscription**

   Operators discover FF-ICE APIs in the Developer Portal, review specifications, and submit subscription requests for approval.

2. **Testing & Transition**

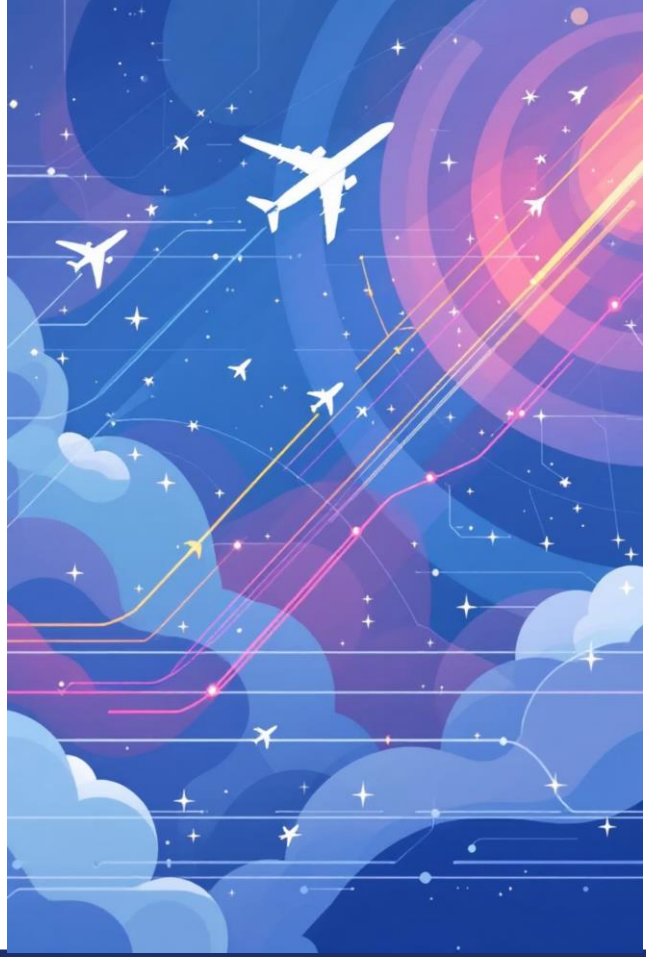
   Integration testing in dev-test validates FIXM schema compliance before promotion to production environment.

3. **Authentication & Control**

   mTLS certificates enforce authentication. Gateway policies validate operator authorization for flight plan submissions.

4. **Monitoring & Validation**

   Real-time analytics track usage patterns. Schema validation at the Gateway ensures FIXM compliance before backend processing.



Conclusion

- FAA is implementing an API Management solution and collaborating with global partners on API Gateway frameworks for Request-Reply messaging.
- **SWIM API Gateway concepts will continue to be explored through:**
  - SIPG Task 3 (Messaging)
  - SIPG Task 7 (Registry/Governance)
  - APAC TF meetings
  - ICAO SWIM forums (e.g., IMP)
- Global ICAO provisions should specify the service description, discovery, and access requirements that enable interoperability
- States and organizations should retain flexibility to choose implementation approaches

Action by the Meeting

- ❑ Include API Governance Framework and guidance materials development in the Governance Working Group
- ❑ Collaborate in SIPG and related APAC Task Force API Gateway strategy discussions and demonstrations
- ❑ Note the information contained in this paper and provide feedback
- ❑ Discuss any relevant matter as appropriate