IEF™
Information Exchange Framework™

INFORMATION EXCHANGE FRAMEWORK (IEF)

Information Exchange Packaging Policy Vocabulary (IEPPV)

Introduction

The Information Exchange Framework™ (IEF™) is an Object Management Group® initiative to establish a family of specifications to enable responsible information sharing and safeguarding (ISS) capabilities for: email exchange, file sharing, instant messaging (chat), structured messaging, and web services.

The first in the family of IEF specifications has been published—the Information Exchange Packaging Policy Vocabulary™ (IEPPV™). This specification provides a policy vocabulary and UML® profile for modeling the rules to securely package and process structured information elements such as: National Information Exchange Model (NIEM), Structured Threat Information eXpression (STIX™), Cyber Observable eXpression (CybOX™), and Trusted Automated eXchange of Indicator Information (TAXII™).

The Information Exchange Packaging Policy Vocabulary establishes a common vocabulary and UML profile for expressing Information and Safeguarding policy (rules and constraints) in a manner that can be serialized and executed by automated services at runtime.

The vocabulary and profile capture user specifications for how structured data is:

- Packaged for release:
  - Assembled (Aggregated, Transformed, Marked & Redacted)
  - Structured
  - Formatted
  - Released to specified distribution channels
- Processed on Receipt:
  - Parsed
  - Mapped and Transformed
  - Marshaled

Using a model-based approach aligned with the Unified Architecture Framework® Profile ensures that:

- Information is released to each recipient, community, or distribution channel in accordance with mission or business, information, system and security architectures.
- Information Sharing Requirements are documented and traceable to business requirements (e.g., policy) and other architectural domains.
- Information exchange specifications and policy models (data patterns) can be reused and shared across projects, operations and missions in order to reduce life-cycle cost and risk.
- Provide architectural metadata that enables threat-risk analysis, and auditability.
- Institutional knowledge is retained.

Value Proposition

- **Platform independence:** The IEPPV may be implemented using one or more vendor products and services that can be integrated through standardized interfaces, messages and protocols.
- **Defense-in-depth:** The IEPPV enables the specification of safeguards (e.g., marking, redaction, transformation (e.g., encryption) to individual data and information elements based on their individual level of sensitivity (e.g., private, confidential, legally-significant, or classified).
- **Policy driven:** The IEPPV uses standard architecture modeling profiles to translate and transform policy instruments (e.g., legislation, regulation, operating procedures, memoranda of understanding, and service–level agreements) into machine-readable rules and constraints.
- **Data centric:** An IEPPV specifies rules and constraints at the data and/or information level.

The IEPPV can be used:

- As a stand-alone set of models to document user requirements for a development team.
- In conduction with Model Driven Architecture® Transformation to automate the transition of interface definitions from business to operations.
- In conjunction with enterprise architecture frameworks and tools, via UAF®, to integration detailed interface specifications with interfaces, systems, platforms, capabilities and organizations.
- In conjunction with analytic tools to assess the threats and risks associated with information sharing patterns across the enterprise.

There is a high cost and risk with current practices for developing and maintaining information sharing and safeguarding capabilities. The IEPPV provides the ability to reduce life-cycle costs and risks by:

- Informing ISS decision making, operational planning, and coordination.
- Improving organizational ability to use information as a resource or force multiplier: do more with fewer resources.
- Enhancing flexibility, agility, and adaptability in ISS capability development.

In summary, the IEPPV addresses the concerns of a broad set of communities that need to simultaneously share and safeguard information, including but not limited to: national security, public safety, healthcare, and government, financial and business services.

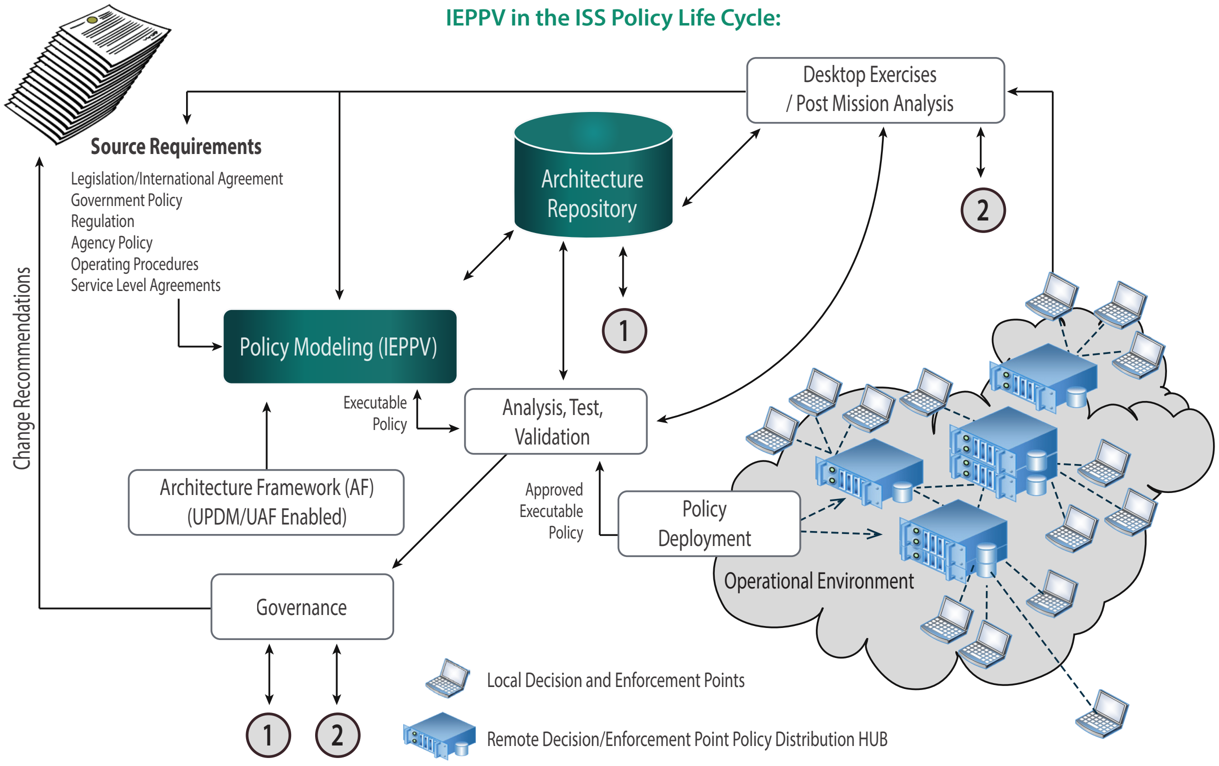
Next Step

We are happy to discuss how OMG membership will benefit your organization. Explore our website at **www.omg.org** and when you are ready, please contact **bd-team@omg.org** or call + 1-781-444-0404 to get started.

About OMG

The Object Management Group® (OMG®) is an international, open membership, not-for-profit computer industry standards consortium with representation from government, industry and academia. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries. OMG modeling standards enable powerful visual design, execution and maintenance of software and other processes. Visit **www.omg.org** for more information.

IEPPV in the ISS Policy Life Cycle:


Source Requirements
Legislation/International Agreement
Government Policy
Regulation
Agency Policy
Operating Procedures
Service Level Agreements
Architecture Repository
Desktop Exercises / Post Mission Analysis
2
1
Change Recommendations
Policy Modeling (IEPPV)
Executable Policy
Analysis, Test, Validation
Architecture Framework (AF) (UPDM/UAF Enabled)
Approved Executable Policy
Policy Deployment
Operational Environment
Governance
1
2
Local Decision and Enforcement Points
Remote Decision/Enforcement Point Policy Distribution HUB