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

The first in the envisioned family of IEF specifications has been published—the Information Exchange Packaging Policy Vocabulary™ (IEPPV™). This specification provides a policy vocabulary and UML® profile model for secure packaging and processing of 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 IEF Reference Architecture, a specification in development, will establish a framework for integrating ISS services into a user’s Technical Architecture. This will ensure:

- Access and release controls reflect the sensitivity of each data and information element, not simply the domain in which it resides.
- Every request for and exchange of information is gated through a policy enforcement point that enforces user–specified ISS policy.
- Information Content is assembled, marked, and packaged in accordance with the data-owner’s policies for a recipient/community based on individual authorizations and privileges.
- Protection mechanisms are applied in accordance with user–specified policies.
- Transactions are recorded in a tamper-resistant log to enable real-time monitoring and forensic auditing.
- Users can dynamically adapt ISS policies and controls based on variations in operational context (e.g., threat, risk, policy, location, and roles & responsibilities) and in accordance with security policy.

Simple View IEF Scope

- Platform independence: The IEF 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 IEF supports layering of information safeguards that automate user-defined ISS policies, e.g., rules and constraints, for each information element based on its designated sensitivity.
- Policy driven: The IEF uses standard architecture modeling profiles to translate policy instruments (e.g., legislation, regulation, operating procedures, memoranda of understanding, and service–level agreements) into machine readable rules and constraints ingested and enforced by IEF-conformant services.
- Data centric: An IEF-conformant service enforces policies based on data and metadata content.
The IEF targets mission domains challenged by wide variations in ISS requirements, multiple internal and external partners, significant security concerns and rapid, often unpredictable, changes in operational contexts (e.g., threat, risk, roles & responsibilities, coalition membership, scale, scope and severity). These information domains (e.g., data/information, applications, platforms and networks) are often logically and physically separated into security enclaves in order to protect sensitive (e.g., classified, confidential, private and legally significant) information. This separation isolates information elements, often making them inaccessible and of little or no value to decision makers.

There is a high cost to maintaining separate security enclaves. A significant number of agencies want to consolidate and integrate their systems and platforms within a single network to enable responsible information sharing:

- to improve decision making, operational planning, coordination and execution.
- to use information as capability resource or force multiplier: do more with fewer resources.
- to enhance flexibility, agility, and adaptability.

In summary, the IEF 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.

Want to learn more?

We are happy to discuss how OMG membership will benefit your organization. Explore our website at [www.omg.org](http://www.omg.org) and when you are ready, please contact [bd-team@omg.org](mailto: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’s modeling standards enable powerful visual design, execution and maintenance of software and other processes. Visit [www.omg.org](http://www.omg.org) for more information.

IEF System Use Case

For a listing of all OMG trademarks, visit [www.omg.org/legal/tm_list.htm](http://www.omg.org/legal/tm_list.htm). All other trademarks are the property of their respective owners.