Objective of this RFP

The Information Exchange Framework (IEF) Policy-based Packaging Service (PS) will provide organizations an automated way to apply user-defined policies that govern the sharing and protection of information. Information exchange policies will be described in accordance with the Information Exchange Policy Vocabulary (IEPV) (Request for Proposal (RFP): mars/2011-03-15).

This RFP solicits proposals for a service specification describing the application-visible interface(s) and behavior of the packaging services. This
includes services for data aggregation and marshalling; data guarding and filtering; syntactic and semantic validation; tag and label processing; data transformation; release control; and routing. The proposals should describe how the service interacts with the middleware and communication networks. In addition, it should address issues related to security, privacy, Quality of Service (QoS), logging, and auditing.

For further details see Chapter 6 of this document.

1.0 Introduction

1.1 Goals of OMG

The Object Management Group (OMG) is the world's largest software consortium with an international membership of vendors, developers, and end users. Established in 1989, its mission is to help computer users solve enterprise integration problems by supplying open, vendor-neutral portability, interoperability and reusability specifications based on Model Driven Architecture (MDA). MDA defines an approach to IT system specification that separates the specification of system functionality from the specification of the implementation of that functionality on a specific technology platform, and provides a set of guidelines for structuring specifications expressed as models. OMG has established numerous widely used standards such as OMG IDL[IDL], CORBA[CORBA], Realtime CORBA [CORBA], GIOP/IIOP[CORBA], UML[UML], MOF[MOF], XMI[XMI] and CWM[CWM] to name a few significant ones.

1.2 Organization of this document

The remainder of this document is organized as follows:

Chapter 2 - Architectural Context - background information on OMG’s Model Driven Architecture.

Chapter 3 - Adoption Process - background information on the OMG specification adoption process.

Chapter 4 - Instructions for Submitters - explanation of how to make a submission to this RFP.

Chapter 5 - General Requirements on Proposals - requirements and evaluation criteria that apply to all proposals submitted to OMG.
Chapter 6 - Specific Requirements on Proposals - problem statement, scope of proposals sought, requirements and optional features, issues to be discussed, evaluation criteria, and timetable that apply specifically to this RFP.

Appendix A – References and Glossary Specific to this RFP

Appendix B – General References and Glossary

1.3 Conventions

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 [RFC2119].

1.4 Contact Information

Questions related to the OMG’s technology adoption process may be directed to omg-process@omg.org. General questions about this RFP may be sent to responses@omg.org.

OMG documents (and information about the OMG in general) can be obtained from the OMG’s web site (http://www.omg.org). OMG documents may also be obtained by contacting OMG at documents@omg.org. Templates for RFPs (like this document) and other standard OMG documents can be found at the OMG Template Downloads Page at http://www.omg.org/technology/template_download.htm

2.0 Architectural Context

MDA provides a set of guidelines for structuring specifications expressed as models and the mappings between those models. The MDA initiative and the standards that support it allow the same model specifying business system or application functionality and behavior to be realized on multiple platforms. MDA enables different applications to be integrated by explicitly relating their models; this facilitates integration and interoperability and supports system evolution (deployment choices) as platform technologies change. The three primary goals of MDA are portability, interoperability and reusability.

Portability of any subsystem is relative to the subsystems on which it depends. The collection of subsystems that a given subsystem depends upon is often loosely called the platform, which supports that subsystem. Portability – and reusability - of such a subsystem is enabled if all the subsystems that it depends upon use standardized interfaces (APIs) and usage patterns.
MDA provides a pattern comprising a portable subsystem that is able to use any one of multiple specific implementations of a platform. This pattern is repeatedly usable in the specification of systems. The five important concepts related to this pattern are:

1. **Model** – A model is a representation of a part of the function, structure and/or behavior of an application or system. A representation is said to be formal when it is based on a language that has a well-defined form (“syntax”), meaning (“semantics”), and possibly rules of analysis, inference, or proof for its constructs. The syntax may be graphical or textual. The semantics might be defined, more or less formally, in terms of things observed in the world being described (e.g. message sends and replies, object states and state changes, etc.), or by translating higher-level language constructs into other constructs that have a well-defined meaning. The optional rules of inference define what unstated properties you can deduce from the explicit statements in the model. In MDA, a representation that is not formal in this sense is not a model. Thus, a diagram with boxes and lines and arrows that is not supported by a definition of the meaning of a box, and the meaning of a line and of an arrow is not a model—it is just an informal diagram.

2. **Platform** – A set of subsystems/technologies that provide a coherent set of functionality through interfaces and specified usage patterns that any subsystem that depends on the platform can use without concern for the details of how the functionality provided by the platform is implemented.

3. **Platform Independent Model (PIM)** – A model of a subsystem that contains no information specific to the platform, or the technology that is used to realize it.

4. **Platform Specific Model (PSM)** – A model of a subsystem that includes information about the specific technology that is used in the realization of that subsystem on a specific platform, and hence possibly contains elements that are specific to the platform.

5. **Mapping** – Specification of a mechanism for transforming the elements of a model conforming to a particular metamodel into elements of another model that conforms to another (possibly the same) metamodel. A mapping may be expressed as associations, constraints, rules, templates with parameters that must be assigned during the mapping, or other forms yet to be determined.

For example, in case of CORBA the platform is specified by a set of interfaces and usage patterns that constitute the CORBA Core Specification [CORBA]. The CORBA platform is independent of operating systems and programming languages. The OMG Trading Object Service specification [TOS] (consisting of
interface specifications in OMG Interface Definition Language (OMG IDL)) can be considered to be a PIM from the viewpoint of CORBA, because it is independent of operating systems and programming languages. When the IDL to C++ Language Mapping specification is applied to the Trading Service PIM, the C++-specific result can be considered to be a PSM for the Trading Service, where the platform is the C++ language and the C++ ORB implementation. Thus the IDL to C++ Language Mapping specification [IDLC++] determines the mapping from the Trading Service PIM to the Trading Service PSM.

Note that the Trading Service model expressed in IDL is a PSM relative to the CORBA platform too. This highlights the fact that platform-independence and platform-specificity are relative concepts.

The UML Profile for EDOC specification [EDOC] is another example of the application of various aspects of MDA. It defines a set of modeling constructs that are independent of middleware platforms such as EJB [EJB], CCM [CCM], MQSeries [MQS], etc. A PIM based on the EDOC profile uses the middleware-independent constructs defined by the profile and thus is middleware-independent. In addition, the specification defines formal metamodels for some specific middleware platforms such as EJB, supplementing the already-existing OMG metamodel of CCM (CORBA Component Model). The specification also defines mappings from the EDOC profile to the middleware metamodels. For example, it defines a mapping from the EDOC profile to EJB. The mapping specifications facilitate the transformation of any EDOC-based PIM into a corresponding PSM for any of the specific platforms for which a mapping is specified.

Continuing with this example, one of the PSMs corresponding to the EDOC PIM could be for the CORBA platform. This PSM then potentially constitutes a PIM, corresponding to which there would be implementation language specific PSMs derived via the CORBA language mappings, thus illustrating recursive use of the Platform-PIM-PSM-Mapping pattern.

Note that the EDOC profile can also be considered to be a platform in its own right. Thus, a model expressed via the profile is a PSM relative to the EDOC platform.

An analogous set of concepts apply to Interoperability Protocols wherein there is a PIM of the payload data and a PIM of the interactions that cause the data to find its way from one place to another. These then are realized in specific ways for specific platforms in the corresponding PSMs.

Analogously, in case of databases there could be a PIM of the data (say using the Relational Data Model), and corresponding PSMs specifying how the data is
OMG adopts standard specifications of models that exploit the MDA pattern to facilitate portability, interoperability and reusability, either through ab initio development of standards or by reference to existing standards. Some examples of OMG adopted specifications are:

1. **Languages** – e.g. IDL for interface specification, UML for model specification, OCL for constraint specification, etc.

2. **Mappings** – e.g. Mapping of OMG IDL to specific implementation languages (CORBA PIM to Implementation Language PSMs), UML Profile for EDOC (PIM) to CCM (CORBA PSM) and EJB (Java PSM), CORBA (PSM) to COM (PSM) etc.

3. **Services** – e.g. Naming Service [NS], Transaction Service [OTS], Security Service [SEC], Trading Object Service [TOS] etc.

4. **Platforms** – e.g. CORBA [CORBA].

5. **Protocols** – e.g. GIOP/IIOP [CORBA] (both structure and exchange protocol), XML Metadata Interchange [XMI] (structure specification usable as payload on multiple exchange protocols).

6. **Domain Specific Standards** – e.g. Data Acquisition from Industrial Systems (Manufacturing) [DAIS], General Ledger Specification (Finance) [GLS], Air Traffic Control (Transportation) [ATC], Gene Expression (Life Science Research) [GE], Personal Identification Service (Healthcare) [PIDS], etc.

For an introduction to MDA, see [MDAa]. For a discourse on the details of MDA please refer to [MDAc]. To see an example of the application of MDA see [MDAb]. For general information on MDA, see [MDAd].

Object Management Architecture (OMA) is a distributed object computing platform architecture within MDA that is related to ISO’s Reference Model of Open Distributed Processing RM-ODP [RM-ODP]. CORBA and any extensions to it are based on OMA. For information on OMA see [OMA].
3.0 Adoption Process

3.1 Introduction

OMG adopts specifications by explicit vote on a technology-by-technology basis. The specifications selected each satisfy the architectural vision of MDA. OMG bases its decisions on both business and technical considerations. Once a specification adoption is finalized by OMG, it is made available for use by both OMG members and non-members alike.

Request for Proposals (RFP) are issued by a Technology Committee (TC), typically upon the recommendation of a Task Force (TF) and duly endorsed by the Architecture Board (AB).

Submissions to RFPs are evaluated by the TF that initiated the RFP. Selected specifications are recommended to the parent TC after being reviewed for technical merit and consistency with MDA and other adopted specifications and endorsed by the AB. The parent TC of the initiating TF then votes to recommend adoption to the OMG Board of Directors (BoD). The BoD acts on the recommendation to complete the adoption process.


3.2 Steps in the Adoption Process

A TF, its parent TC, the AB and the Board of Directors participate in a collaborative process, which typically takes the following form:

- **Development and Issuance of RFP**

  RFPs are drafted by one or more OMG members who are interested in the adoption of a standard in some specific area. The draft RFP is presented to an appropriate TF, based on its subject area, for approval and recommendation to issue. The TF and the AB provide guidance to the drafters of the RFP. When the TF and the AB are satisfied that the RFP is appropriate and ready for issuance, the TF recommends issuance to its parent TC, and the AB endorses the recommendation. The TC then acts on the recommendation and issues the RFP.

- **Letter of Intent (LOI)**

  A Letter of Intent (LOI) must be submitted to the OMG signed by an officer of the member organization which intends to respond to the RFP, confirming
the organization’s willingness to comply with OMG’s terms and conditions, and commercial availability requirements. (See section 4.3 for more information.). In order to respond to an RFP the organization must be a member of the TC that issued the RFP.

- **Voter Registration**

Interested OMG members, other than Trial, Press and Analyst members, may participate in specification selection votes in the TF for an RFP. They may need to register to do so, if so stated in the RFP. Registration ends on a specified date, 6 or more weeks after the announcement of the registration period. The registration closure date is typically around the time of initial submissions. Member organizations that have submitted an LOI are automatically registered to vote.

- **Initial Submissions**

Initial Submissions are due by a specified deadline. Submitters normally present their proposals at the first meeting of the TF after the deadline. Initial Submissions are expected to be complete enough to provide insight on the technical directions and content of the proposals.

- **Revision Phase**

During this time submitters have the opportunity to revise their Submissions, if they so choose.

- **Revised Submissions**

Revised Submissions are due by a specified deadline. Submitters again normally present their proposals at the next meeting of the TF after the deadline. (Note that there may be more than one Revised Submission deadline. The decision to set new Revised Submission deadlines is made by the registered voters for that RFP.)

- **Selection Votes**

When the registered voters for the RFP believe that they sufficiently understand the relative merits of the Revised Submissions, a selection vote is taken. The result of this selection vote is a recommendation for adoption to the TC. The AB reviews the proposal for MDA compliance and technical merit. An endorsement from the AB moves the voting process into the issuing Technology Committee. An eight-week voting period ensues in which the TC votes to recommend adoption to the OMG Board of Directors (BoD). The final vote, the vote to adopt, is taken by the BoD and is based on technical merit as well as business qualifications. The resulting draft standard is called the *Alpha Specification*. 
• Business Committee Questionnaire

The submitting members whose proposal is recommended for adoption need to submit their response to the BoD Business Committee Questionnaire [BCQ] detailing how they plan to make use of and/or make the resulting standard available in products. If no organization commits to make use of the standard, then the BoD will typically not act on the recommendation to adopt the standard - so it is very important to fulfill this requirement.

• Finalization

A Finalization Task Force (FTF) is chartered by the TC that issued the RFP, to prepare an Alpha submission for publishing as a Formal (i.e. publicly available) specification, by fixing any problems that are reported by early users of the specification. Upon completion of its activity the FTF recommends adoption of the resulting Beta (draft) specification. The parent TC acts on the recommendation and recommends adoption to the BoD. OMG Technical Editors produce the Formal Specification document based on this Beta Specification.

• Revision

A Revision Task Force (RTF) is normally chartered by a TC, after the FTF completes its work, to manage issues filed against the Formal Specification by implementers and users. The output of the RTF is a Beta specification reflecting minor technical changes, which the TC and Board will usually approve for adoption as the next version of the Formal Specification.

3.3 Goals of the evaluation

The primary goals of the TF evaluation are to:

• Provide a fair and open process
• Facilitate critical review of the submissions by members of OMG
• Provide feedback to submitters enabling them to address concerns in their revised submissions
• Build consensus on acceptable solutions
• Enable voting members to make an informed selection decision

Submitters are expected to actively contribute to the evaluation process.
4.0 Instructions for Submitters

4.1 OMG Membership

To submit to an RFP issued by the Platform Technology Committee the submitter or submitters must be either Platform or Contributing members on the date of the submission deadline, while for Domain Technology RFPs the submitter or submitters must be either Contributing or Domain members. Submitters sometimes choose to name other organizations that support a submission in some way; however, this has no formal status within the OMG process, and for OMG’s purposes confers neither duties nor privileges on the organizations thus named.

4.2 Submission Effort

An RFP submission may require significant effort in terms of document preparation, presentations to the issuing TF, and participation in the TF evaluation process. Several staff months of effort might be necessary. OMG is unable to reimburse submitters for any costs in conjunction with their submissions to this RFP.

4.3 Letter of Intent

A Letter of Intent (LOI) must be submitted to the OMG Business Committee signed by an officer of the submitting organization signifying its intent to respond to the RFP and confirming the organization’s willingness to comply with OMG’s terms and conditions, and commercial availability requirements. These terms, conditions, and requirements are defined in the Business Committee RFP Attachment and are reproduced verbatim in section 4.4 below.

The LOI should designate a single contact point within the submitting organization for receipt of all subsequent information regarding this RFP and the submission. The name of this contact will be made available to all OMG members. The LOI is typically due 60 days before the deadline for initial submissions. LOIs must be sent by fax or paper mail to the “RFP Submissions Desk” at the main OMG address shown on the first page of this RFP.

Here is a suggested template for the Letter of Intent:

This letter confirms the intent of <organization required> (the organization) to submit a response to the OMG <RFP name required> RFP. We will grant OMG and its members the right to copy our response for review purposes as specified in section 4.7 of the RFP. Should our response be adopted by OMG we will comply with the OMG Business Committee terms set out in section 4.4 of the RFP and in document omg/06-03-02.
<contact name and details required> will be responsible for liaison with OMG regarding this RFP response.

The signatory below is an officer of the organization and has the approval and authority to make this commitment on behalf of the organization.

<signature required>

4.4 Business Committee RFP Attachment

This section contains the text of the Business Committee RFP attachment concerning commercial availability requirements placed on submissions. This attachment is available separately as an OMG document omg/06-03-02.

Commercial considerations in OMG technology adoption

4.5 A1 Introduction

OMG wishes to encourage rapid commercial adoption of the specifications it publishes. To this end, there must be neither technical, legal nor commercial obstacles to their implementation. Freedom from the first is largely judged through technical review by the relevant OMG Technology Committees; the second two are the responsibility of the OMG Business Committee. The BC also looks for evidence of a commitment by a submitter to the commercial success of products based on the submission.

4.6 A2 Business Committee evaluation criteria

4.6.1 A2.1 Viable to implement across platforms

While it is understood that final candidate OMG submissions often combine technologies before they have all been implemented in one system, the Business Committee nevertheless wishes to see evidence that each major feature has been implemented, preferably more than once, and by separate organisations. Pre-product implementations are acceptable. Since use of OMG specifications should not be dependant on any one platform, cross-platform availability and interoperability of implementations should be also be demonstrated.
4.6.2 A2.2 Commercial availability

In addition to demonstrating the existence of implementations of the specification, the submitter must also show that products based on the specification are commercially available, or will be within 12 months of the date when the specification was recommended for adoption by the appropriate Task Force. Proof of intent to ship product within 12 months might include:

- A public product announcement with a shipping date within the time limit.
- Demonstration of a prototype implementation and accompanying draft user documentation.

Alternatively, and at the Business Committee's discretion, submissions may be adopted where the submitter is not a commercial software provider, and therefore will not make implementations commercially available. However, in this case the BC will require concrete evidence of two or more independent implementations of the specification being used by end-user organisations as part of their businesses. Regardless of which requirement is in use, the submitter must inform the OMG of completion of the implementations when commercially available.

4.6.3 A2.3 Access to Intellectual Property Rights

OMG will not adopt a specification if OMG is aware of any submitter, member or third party which holds a patent, copyright or other intellectual property right (collectively referred to in this policy statement as "IPR") which might be infringed by implementation or recommendation of such specification, unless OMG believes that such IPR owner will grant a license to organisations (whether OMG members or not) on non-discriminatory and commercially reasonable terms which wish to make use of the specification. Accordingly, the submitter must certify that it is not aware of any claim that the specification infringes any IPR of a third party or that it is aware and believes that an appropriate non-discriminatory license is available from that third party. Except for this certification, the submitter will not be required to make any other warranty, and specifications will be offered by OMG for use "as is". If the submitter owns IPR to which an use of a specification based upon its submission would necessarily be subject, it must certify to the Business Committee that it will make a suitable license available to any user on non-discriminatory and commercially reasonable terms, to permit development and commercialisation of an implementation that includes such IPR.

It is the goal of the OMG to make all of its technology available with as few impediments and disincentives to adoption as possible, and therefore OMG strongly encourages the submission of technology as to which royalty-free
licenses will be available. However, in all events, the submitter shall also certify that any necessary licence will be made available on commercially reasonable, non-discriminatory terms. The submitter is responsible for disclosing in detail all known restrictions, placed either by the submitter or, if known, others, on technology necessary for any use of the specification.

4.6.4 A2.4 Publication of the specification

Should the submission be adopted, the submitter must grant OMG (and its sublicensees) a world-wide, royalty-free licence to edit, store, duplicate and distribute both the specification and works derived from it (such as revisions and teaching materials). This requirement applies only to the written specification, not to any implementation of it.

4.6.5 A2.5 Continuing support

The submitter must show a commitment to continue supporting the technology underlying the specification after OMG adoption, for instance by showing the BC development plans for future revisions, enhancement or maintenance.

4.7 Responding to RFP items

4.7.1 Complete proposals

A submission must propose full specifications for all of the relevant requirements detailed in Chapter 6 of this RFP. Submissions that do not present complete proposals may be at a disadvantage.

Submitters are highly encouraged to propose solutions to any optional requirements enumerated in Chapter 6.

4.7.2 Additional specifications

Submissions may include additional specifications for items not covered by the RFP that they believe to be necessary and integral to their proposal. Information on these additional items should be clearly distinguished.

Submitters must give a detailed rationale as to why these specifications should also be considered for adoption. However submitters should note that a TF is unlikely to consider additional items that are already on the roadmap of an OMG TF, since this would pre-empt the normal adoption process.
4.7.3 Alternative approaches

Submitters may provide alternative RFP item definitions, categorizations, and groupings so long as the rationale for doing so is clearly stated. Equally, submitters may provide alternative models for how items are provided if there are compelling technological reasons for a different approach.

4.8 Confidential and Proprietary Information

The OMG specification adoption process is an open process. Responses to this RFP become public documents of the OMG and are available to members and non-members alike for perusal. No confidential or proprietary information of any kind will be accepted in a submission to this RFP.

4.9 Copyright Waiver

Every submission document must contain: (i) a waiver of copyright for unlimited duplication by the OMG, and (ii) a limited waiver of copyright that allows each OMG member to make up to fifty (50) copies of the document for review purposes only. See Section 4.9.2 for recommended language.

4.10 Proof of Concept

Submissions must include a “proof of concept” statement, explaining how the submitted specifications have been demonstrated to be technically viable. The technical viability has to do with the state of development and maturity of the technology on which a submission is based. This is not the same as commercial availability. Proof of concept statements can contain any information deemed relevant by the submitter; for example:

“This specification has completed the design phase and is in the process of being prototyped.”

“An implementation of this specification has been in beta-test for 4 months.”

“A named product (with a specified customer base) is a realization of this specification.”

It is incumbent upon submitters to demonstrate the technical viability of their proposal to the satisfaction of the TF managing the evaluation process. OMG will favor proposals based on technology for which sufficient relevant experience has been gained.
4.11 Format of RFP Submissions

This section presents the structure of a submission in response to an RFP. All submissions must contain the elements itemized in section 4.9.2 below before they can be accepted as a valid response for evaluation or a vote can be taken to recommend for adoption.

4.11.1 General

- Submissions that are concise and easy to read will inevitably receive more consideration.

- Submitted documentation should be confined to that directly relevant to the items requested in the RFP. If this is not practical, submitters must make clear what portion of the documentation pertains directly to the RFP and what portion does not.

- The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" shall be used in the submissions with the meanings as described in RFC 2119 [RFC2119].

4.11.2 Required Outline

A three-part structure for submissions is required. Part I is non-normative, providing information relevant to the evaluation of the proposed specification. Part II is normative, representing the proposed specification. Specific sections like Appendices may be explicitly identified as non-normative in Part II. Part III is normative specifying changes that must be made to previously adopted specifications in order to be able to implement the specification proposed in Part II.

PART I

- A cover page carrying the following information (a template for this is available [Inventory]):
  - The full name of the submission
  - The primary contact for the submission
  - The acronym proposed for the specification (e.g. UML, CORBA)
  - The name and document number of the RFP to which this is a response
  - The document number of the main submission document
- An inventory of all accompanying documents, with OMG document number, short description, a URL where appropriate, and whether they are normative.

- List of OMG members making the submission (see 4.1) listing exactly which members are making the submission, so that submitters can be matched with LOI responders and their current eligibility can be verified.

- Copyright waiver (see 4.7), in a form acceptable to the OMG.

One acceptable form is:

“Each of the entities listed above: (i) grants to the Object Management Group, Inc. (OMG) a nonexclusive, royalty-free, paid up, worldwide license to copy and distribute this document and to modify this document and distribute copies of the modified version, and (ii) grants to each member of the OMG a nonexclusive, royalty-free, paid up, worldwide license to make up to fifty (50) copies of this document for internal review purposes only and not for distribution, and (iii) has agreed that no person shall be deemed to have infringed the copyright in the included material of any such copyright holder by reason of having used any OMG specification that may be based hereon or having conformed any computer software to such specification.”

If you wish to use some other form you must get it approved by the OMG legal counsel before using it in a submission.

- For each member making the submission, an individual contact point who is authorized by the member to officially state the member’s position relative to the submission, including matters related to copyright ownership, etc. (see 4.3)

- Overview or guide to the material in the submission

- Overall design rationale (if appropriate)

- Statement of proof of concept (see 4.8)

- Resolution of RFP requirements and requests

   Explain how the proposal satisfies the specific requirements and (if applicable) requests stated in Chapter 6. References to supporting material in Part II should be given.

   In addition, if the proposal does not satisfy any of the general requirements stated in Chapter 5, provide a detailed rationale.

- Responses to RFP issues to be discussed
Discuss each of the “Issues To Be Discussed” identified in Chapter 6.

PART II

The contents of this part should be structured based on the template found in [FORMS] and should contain the following elements as per the instructions in the template document cited above:

- Scope of the proposed specification
- Proposed conformance criteria
  Submissions should propose appropriate conformance criteria for implementations.
- Proposed normative references
  Submissions should provide a list of the normative references that are used by the proposed specification
- Proposed list of terms and definitions
  Submissions should provide a list of terms that are used in the proposed specification with their definitions.
- Proposed list of symbols
  Submissions should provide a list of special symbols that are used in the proposed specification together with their significance
- Proposed specification

PART III

- Changes or extensions required to existing OMG specifications
  Submissions must include a full specification of any changes or extensions required to existing OMG specifications. This should be in a form that enables “mechanical” section-by-section revision of the existing specification.

4.12 How to Submit

Submitters should send an electronic version of their submission to the RFP Submissions Desk (omg-documents@omg.org) at OMG Headquarters by 5:00 PM U.S. Eastern Standard Time (22:00 GMT) on the day of the Initial and Revised Submission deadlines. Acceptable formats are Adobe FrameMaker source, ODF (ISO/IEC 26300), OASIS Darwin Information Typing Architecture (DITA) or OASIS DocBook 4.x (or later).
Submitters should make sure they receive electronic or voice confirmation of the successful receipt of their submission. Submitters should be prepared to send a single hardcopy version of their submission, if requested by OMG staff, to the attention of the “RFP Submissions Desk” at the main OMG address shown on the first page of this RFP.
5.0 General Requirements on Proposals

5.1 Requirements

5.1.1 Submitters are encouraged to express models using OMG modeling languages such as UML, MOF, CWM and SPEM (subject to any further constraints on the types of the models and modeling technologies specified in Chapter 6 of this RFP). Submissions containing models expressed via OMG modeling languages shall be accompanied by an OMG XMI [XMI] representation of the models (including a machine-readable copy). A best effort should be made to provide an OMG XMI representation even in those cases where models are expressed via non-OMG modeling languages.

5.1.2 Chapter 6 of this RFP specifies whether PIM(s), PSM(s), or both are being solicited. If proposals specify a PIM and corresponding PSM(s), then the rules specifying the mapping(s) between the PIM and PSM(s) shall either be identified by reference to a standard mapping or specified in the proposal. In order to allow possible inconsistencies in a proposal to be resolved later, proposals shall identify whether the mapping technique or the resulting PSM(s) are to be considered normative.

5.1.3 Proposals shall be precise and functionally complete. All relevant assumptions and context required for implementing the specification shall be provided.

5.1.4 Proposals shall specify conformance criteria that clearly state what features all implementations must support and which features (if any) may optionally be supported.

5.1.5 Proposals shall reuse existing OMG and other standard specifications in preference to defining new models to specify similar functionality.

5.1.6 Proposals shall justify and fully specify any changes or extensions required to existing OMG specifications. In general, OMG favors proposals that are upwards compatible with existing standards and that minimize changes and extensions to existing specifications.

5.1.7 Proposals shall factor out functionality that could be used in different contexts and specify their models, interfaces, etc. separately. Such minimalism fosters re-use and avoids functional duplication.
5.1.8 Proposals shall use or depend on other specifications only where it is actually necessary. While re-use of existing specifications to avoid duplication will be encouraged, proposals should avoid gratuitous use.

5.1.9 Proposals shall be compatible with and usable with existing specifications from OMG and other standards bodies, as appropriate. Separate specifications offering distinct functionality should be usable together where it makes sense to do so.

5.1.10 Proposals shall preserve maximum implementation flexibility. Implementation descriptions should not be included and proposals shall not constrain implementations any more than is necessary to promote interoperability.

5.1.11 Proposals shall allow independent implementations that are substitutable and interoperable. An implementation should be replaceable by an alternative implementation without requiring changes to any client.

5.1.12 Proposals shall be compatible with the architecture for system distribution defined in ISO’s Reference Model of Open Distributed Processing [RM-ODP]. Where such compatibility is not achieved, or is not appropriate, the response to the RFP must include reasons why compatibility is not appropriate and an outline of any plans to achieve such compatibility in the future.

5.1.13 In order to demonstrate that the specification proposed in response to this RFP can be made secure in environments requiring security, answers to the following questions shall be provided:

- What, if any, are the security sensitive elements that are introduced by the proposal?
- Which accesses to security-sensitive elements must be subject to security policy control?
- Does the proposed service or facility need to be security aware?
- What default policies (e.g., for authentication, audit, authorization, message protection etc.) should be applied to the security sensitive elements introduced by the proposal? Of what security considerations must the implementers of your proposal be aware?

The OMG has adopted several specifications, which cover different aspects of security and provide useful resources in formulating responses. [CSIV2] [SEC] [RAD].
5.1.14 Proposals shall specify the degree of internationalization support that they provide. The degrees of support are as follows:

a) Uncategorized: Internationalization has not been considered.

b) Specific to <region name>: The proposal supports the customs of the specified region only, and is not guaranteed to support the customs of any other region. Any fault or error caused by requesting the services outside of a context in which the customs of the specified region are being consistently followed is the responsibility of the requester.

c) Specific to <multiple region names>: The proposal supports the customs of the specified regions only, and is not guaranteed to support the customs of any other regions. Any fault or error caused by requesting the services outside of a context in which the customs of at least one of the specified regions are being consistently followed is the responsibility of the requester.

d) Explicitly not specific to <region(s) name>: The proposal does not support the customs of the specified region(s). Any fault or error caused by requesting the services in a context in which the customs of the specified region(s) are being followed is the responsibility of the requester.

5.2 Evaluation criteria

Although the OMG adopts model-based specifications and not implementations of those specifications, the technical viability of implementations will be taken into account during the evaluation process. The following criteria will be used:

5.2.1 Performance

Potential implementation trade-offs for performance will be considered.

5.2.2 Portability

The ease of implementation on a variety of systems and software platforms will be considered.

5.2.3 Securability

The answer to questions in section 5.1.13 shall be taken into consideration to ascertain that an implementation of the proposal is securable in an environment requiring security.
5.2.4 Conformance: Inspectability and Testability

The adequacy of proposed specifications for the purposes of conformance inspection and testing will be considered. Specifications should provide sufficient constraints on interfaces and implementation characteristics to ensure that conformance can be unambiguously assessed through both manual inspection and automated testing.

5.2.5 Standardized Metadata

Where proposals incorporate metadata specifications, usage of OMG standard XMI metadata [XMI] representations must be provided as this allows specifications to be easily interchanged between XMI compliant tools and applications. Since use of XML (including XMI and XML/Value [XML/Value]) is evolving rapidly, the use of industry specific XML vocabularies (which may not be XMI compliant) is acceptable where justified.
6.0 Specific Requirements on Proposals

The IEF constitutes a set of interdependent specifications that will enable user communities to define information exchange policies in a manner that can be programmatical enforced. To date, the components of the IEF include:

1. The **Information Exchange Policy Vocabulary (IEPV)**: a standard vocabulary for specifying policies for the publication and processing of information messages (or payloads) conforming to the agreed semantics of the participants to the exchange. The IEPV specification will include one or more language specifications (e.g., UML, XACML, SAML and Ponder) for the policy statements.

2. The **Information Exchange Policy-based Packaging Service (IEPPS)**: ingests Information Exchange Policies (IEP) in one or more of the policy languages defined in the IEPV specification and applies these policies to guide the packaging of messages into a form suitable for subsequent release.

3. The **Information Exchange Policy Management Service (IEPMS)**: supports the creation and management of information policies and allows participants to configure and manage these information policies in a manner that adapts to changes in operational context, participation or information exchange agreements.

The overall goal of the IEF is to separate the rules for exchanging information from the services that enforce those policies. This will allow participants to retain institutional memory and adapt to rapidly changing operational and technical environments.

IEPPS is a service that applies semantic and business rules for static and dynamic aggregation and marshaling of structured information. The IEPPS will interoperate with other IEF services.

Recent discussion with the Department of Homeland Security (DHS) and Project Manager Information Sharing Environment (PM-ISE) indicated the IEF should investigate extending the IEF concepts into the Identify, Credentials and Access Management domain. This expansion will be investigated in future iterations of the IEF.

---

1 IEPV RFP refers to this service as IE Policy Enforcement Service (IEPES).
6.1 Problem Statement

Increasingly, public, private and military organizations are being mandated to share information and collaborate with multiple agencies to deliver operational outcomes. These expanding mandates impose a broad set of often contradictory requirements for organizations: To dynamically expose or share information with selected partners; while at the same time, provide adequate protection for sensitive, private, confidential, classified or legally significant information. It is becoming increasingly clear that the traditional processes for addressing the release and sharing of sensitive information cannot adapt to the increases in operational tempo and the dynamics of real-world events. Nor can operators be relied upon to arbitrate an increasingly complex set information exchange policies. To enable trusted information sharing environments, agencies need to accurately describe the policies for the exchange of information in a manner that can be certified and accredited for use.

Many of the efforts to develop and sustain information sharing environments have fallen short of stakeholder expectations and operational needs. The dynamics of real-world operations and the fluidity and breadth of requirements for shared information and knowledge have demonstrated that traditional Information System development is insufficient to meet community requirements for flexible and agile interoperability solutions. As demonstrated by recent events (e.g., SARS, Tsunamis, the 2007 London subway bombing, the 1998 Ice Storm, Katrina and 9/11), the ability to rapidly align information systems across a broad and diverse infrastructure at the onset of an event is critical to the planning, response and recovery phases of the operation. Further, the ability to rapidly form and reconfigure (based on operational context) communities of interest (CoI) is requisite to developing the shared operational views needed to provide timely and accurate situational awareness and decision support. Interoperable Sharing environments are further challenged by the need to maintain the quality (accuracy, relevancy, timeliness, usability, completeness, perception and trustworthiness) of information and, at the same time, respecting security and privacy constraints.

Many public information systems have evolved as stovepipes (operationally, procedurally and technically), driven by program specific legislation, policy and practices. The extent to which information is or can be shared between parties is restricted, often requiring written requests on a case-by-case basis. At times where information must flow quickly from one agency to another to avoid a disaster or prevent a criminal or terrorist act, existing capabilities are largely inadequate. Collaboration relies more on established personal trust relationships than on operational procedures or interconnected and integrated information systems. These practices do not provide the agility and responsiveness required to react quickly and efficiently to planned or unplanned incidents or threats. Because communication pathways between agencies are not seamless, the information needed to coordinate operations, or business processes, cannot be shared effectively and efficiently. Even when information is accessible, it may be incomplete, inaccurate, late, difficult to interpret, and/or structured in a manner that makes it difficult to use. The problems are further exacerbated by duplicate
or similar data existing in multiple systems, owned by different agencies, or captured and processed for different purposes.

The Middleware and Related Services (MARS) PTF is working with the C4I DTF in the issuance of this RFP. It is also collaborating with other OMG Special Interest Groups (SIGs), Domain Task Forces (DTFs) and Platform Task Forces (PTFs) to address many related requirements and technologies complementing the IEF initiative; including Security, Radio operation and control, Real-time Data Exchange and Quality of Service (QOS). The RFP directs respondents to integrate existing and evolving standards into their submissions for IEF elements, wherever possible.

6.2 Scope of Proposals Sought

This RFP represents the second of three IEF related RFPs to be released by the Middleware and Related Services (MARS) Platform Task Force related to the IEF. The three IEF RFPs include:

1. Information Exchange Policy Vocabulary (IEPV)\(^2\);
2. Information Exchange Policy-based Packaging Service (IEPPS); and
3. Information Exchange Policy Management Service (IEPMS).

Figure 1 provides the contextual relationships between the three RFPs and other participating elements in the IEF.

The overall objective for the IEF is to use policies (expressed in a standard vocabulary across several language specifications) to control the staging and release and receipt of information. The IEPPS will be used to apply message packaging policies conforming to information sharing agreements described using the standardized vocabulary. The policy vocabulary will be defined by the Information Exchange Policy Vocabulary (IEPV) specification (RFP: mars/2011-03-15). The policies will be modified and maintained in accordance with the Information Exchange Policy Management Service (IEPMS)\(^3\).

The IEPPS will incorporate, integrate, and/or interoperate with the following capabilities, depending on the use-cases specified by the submitters:

- One or more information dissemination services, such as DDS, CORBA, or web services.
- IEF Policy Management Service.

In addition, the IEPPS may provide interfaces to other services required by the specific use-cases defined within the submissions. These services may include:

- Identity Management

---

\(^3\) RFP for this service under development
• Credentials Management
• Access Management
• Encryption
• Key Management
• Security Registry
• User Defined Services
• Auditing Services.

6.3 Relationship to other OMG Specifications and activities

6.3.1 Relationship to OMG specifications

The intent is for the submission to maximize the use of existing and evolving OMG standards for at least one of the Platform Specific Models and implementations. MARS is not specifying these relationships; however, submitters are encouraged to identify related internationally or commercially accepted standards to deliver the IEPPS capability. OMG Standards that should be investigated include:

2. Unified Profile for DODAF and MODAF (UPDM: http://www.omg.org/spec/UP2/);
6.3.2 The IEF has a number of potential relationships to other OMG Documents and work in progress. Efforts should be made to incorporate these efforts whenever possible.


6.4 Related non-OMG Activities, Documents and Standards

As with all OMG standards; this RFP is not directing the use or adoption of specific activities, documents and/or standards. However, submitters are encouraged to use related international or commercially accepted standards to deliver the IEF Policy Vocabulary capability.

1. National Information Exchange Model Information Exchange Package Description (IEPD: [http://it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm](http://it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm));


9. The Joint C3 Information Exchange Data Model. [https://mipsite.lsec.dnd.ca/Pages/Default.aspx](https://mipsite.lsec.dnd.ca/Pages/Default.aspx)

10. Logical Entity eXchange Specification (LEXS) [http://130.207.211.107/content/lexs-overview](http://130.207.211.107/content/lexs-overview)


The IEF effort is generally targeting the C4I, Public Safety and Security, and Emergency Management domains. For this reason, there is particular interest in supporting the Extensible Mark-up Language (XML) based exchange standards/specifications developed for these purposes:

1. National Information Exchange Model (NIEM; [http://it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm](http://it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm));

2. Emergency Management Information Standards:
   b. Emergency Data Exchange Language - Distribution Element (EDXL-DE; [http://www.oasis-emergency.org/product/category/edxl-de-10](http://www.oasis-emergency.org/product/category/edxl-de-10)),
   d. Emergency Data Exchange Language - Hospital Availability Exchange (EDXL-HAVE; [http://www.oasis-emergency.org/product/category/edxl-have-10](http://www.oasis-emergency.org/product/category/edxl-have-10)),
   e. Cyclone Warning Markup Language (CWML; [http://www.ogcnetwork.net/node/397](http://www.ogcnetwork.net/node/397)),

Cyclone Warning Markup Language (CWML): [http://www.ogcnetwork.net/node/397](http://www.ogcnetwork.net/node/397)
Information Exchange Policy-based Packaging Service (IEPPS)

3. Geospatial Standards:
   a. GeoRSS (http://www.georss.org/gml),
   b. Geography Markup Language (GML: http://www.opengeospatial.org/standards/gml),
   c. Web Feature Service (WFS: http://www.opengeospatial.org/standards/wfs),
   d. Web Mapping Service (WMS: http://www.opengeospatial.org/standards/wms),
   e. Sensor Observation Service (SOS: http://www.opengeospatial.org/standards/sos),
   f. SensorML (http://www.ogcnetwork.net/SensorML), and
   g. Sensor Planning Service (SPS: http://www.opengeospatial.org/standards/spx);

4. Joint Consultation, Command and Control Information Exchange Data Model (JC3IEMD; https://mipsite.lsec.dnd.ca/Pages/MIPandNATO.aspx);

5. Multilateral Interoperability Program (MIP) XML (https://mipsite.lsec.dnd.ca/Pages/MIPandNATO.aspx);

6. Universal CORE (UCORE: http://dodcio.defense.gov/initiatives/ucore.shtml);

7. C2 CORE (http://dodcio.defense.gov/initiatives/ucore.shtml); and


In addition to these community vocabulary specifications, submitters should use, where applicable, standardized policy languages as part of their Platform Specific Models, such as:

1. OASIS SOA Reference Model (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm);

2. Security Assertion Markup Language 2.0 (SAML 2.0; http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security);

3. eXtensible Access Control Markup Language (XACML 1.0; http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml);

References to the specifications and standards cited in this Section are provided in Annex B.2.

5. Ponder (http://www-dse.doc.ic.ac.uk/Research/policies/ponder.shtml);

6. Simple Knowledge Organization System (SKOS: http://www.w3.org/2009/08/skos-reference/skos.html);

7. ISO 11179-3 Edition 3 (http://metadata-stds.org/11179/); and


The above represents a growing collection of messaging protocols to be addressed by the communities being targeted by this RFP. Services are required to help these communities manage the increasing complexities of their information environments.

6.5 Mandatory Requirements

1. The IEPPS shall accept information exchange policies conforming to one or more of the language profiles defined in the Information Exchange Policy Vocabulary (IEPV) Specification. (This specification is currently under development under the RFP: mars/11-03-15).

2. The IEPPS shall provide an interface that allows active policies to be configured at run-time. The interface will support but not be limited to the following operations:
   a. Import new or modified policies;
   b. Activate existing, new or modified policies;
   c. Deactivate existing policies;
   d. Export policies in a persistent format.

3. The IEPPS shall support the dynamic and static invocations of the operations listed above.

4. The IEPPS shall restrict the release of information messages and content to that specified in active policies.

5. The IEPPS shall release and accept information to one or more selected middleware (e.g. DDS, CORBA, and Web Services).

6. The IEPPS shall record changes to policies.

7. The IEPPS shall record transactions (for both release and receive operations), including the state or results of the transaction (e.g., rejected, incomplete semantic, data error, or success).
8. The IEPPS shall provide an interface to record its operational status.

9. The IEPPS shall provide an interface to report its operational status to external applications.

6.6 Optional Requirements

This section identifies optional requirements considered beneficial to the development and deployment of IEPPS implementations.

1. The IEPPS may provide a PSM that supports enforcement of policies defined for the SOPES Information Exchange Data Model (IEDM).

2. The IEPPS may provide interfaces to interoperate with user specified IEF services and policies. Such services and policies may include:
   - Identity Management
   - Credentials Management
   - Access Management
   - Encryption
   - Key Management
   - Security Registry
   - User Defined Services
   - Auditing Services.

3. The IEPPS may provide interfaces for integration with user applications.

4. The IEPPS may provide interfaces to control resource usage (e.g., thread priority, memory usage, bandwidth).

5. The IEPPS may provide interfaces that support the configuration of recording detail levels: e.g., “None”, “Minimal”, “Normal”, “Detailed”, “Debugging”).

6.7 Issues to be discussed

The proposal(s) shall discuss:

1. Use Cases for operation of the IEPPS

2. Processes for integrating policies (new and/or modified) into the IEPPS prior to and during operations

3. Life cycle issues of active policies
4. Interoperation with the Information Exchange Policy Management Service (IEPMS)

5. Strategies for enforcing policies defined by the SOPES IEDM specification,

6. Strategies for enforcing policies defined by the UML Profile for NIEM and other XML based exchange standards/specifications.

7. Use of IEPPS by standard information dissemination and middleware services and technologies (e.g., DDS, CORBA, or web services).

8. The extent to which IEPPS delivers high levels of flexibility, extensibility, supportability, maintainability and its ability to address dynamic asymmetric real-world operations.

9. Deployment and operation of an IEPPS.

6.8 Evaluation Criteria

More desirable submissions are those that:

1. Support the policies defined in the SOPES IEDM, UML Profile for NIEM, and UPDM;

2. Can be used by multiple information dissemination and/or middleware services and technologies, e.g.: CORBA, DDS, and web services.

3. Demonstrate high flexibility, extensibility, maintainability, supportability and ease of use.

4. Demonstrate versatility and flexibility in operations and deployment.

5. Leverage external information assurance and security mechanisms.

6. Leverage standard data persistence services and technologies.

7. Require few resources such as computer memory, disk space, and processing power.

6.9 Other information unique to this RFP

• None

6.10 RFP Timetable

The timetable for this RFP is given below.

<table>
<thead>
<tr>
<th>Event or Activity</th>
<th>Actual Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation of RFP by TF</td>
<td>November 14, 2011</td>
</tr>
<tr>
<td>RFP placed on OMG document server</td>
<td>November 14, 2011</td>
</tr>
<tr>
<td>Event Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Approval of RFP by Architecture Board</td>
<td>December 15, 2011</td>
</tr>
<tr>
<td>Review by TC</td>
<td></td>
</tr>
<tr>
<td>TC votes to issue RFP</td>
<td>December 16, 2011</td>
</tr>
<tr>
<td>LOI to submit to RFP due</td>
<td>March 19, 2012</td>
</tr>
<tr>
<td>Initial Submissions due and placed on OMG document server (“Four week rule”)</td>
<td>August 13, 2012</td>
</tr>
<tr>
<td>Voter registration closes</td>
<td>September 3, 2011</td>
</tr>
<tr>
<td>Initial Submission presentations</td>
<td>September 10-13, 2012</td>
</tr>
<tr>
<td>Preliminary evaluation by TF</td>
<td>September 10-13, 2012</td>
</tr>
<tr>
<td>Revised Submissions due and placed on OMG document server (“Four week rule”)</td>
<td>November 12, 2012</td>
</tr>
<tr>
<td>Revised Submission presentations</td>
<td>December 10-16, 2012</td>
</tr>
<tr>
<td>Final evaluation and selection by TF</td>
<td>December 17, 2012</td>
</tr>
<tr>
<td>Recommendation to AB and TC</td>
<td></td>
</tr>
<tr>
<td>Approval by Architecture Board</td>
<td>December 14, 2012</td>
</tr>
<tr>
<td>Review by TC</td>
<td></td>
</tr>
<tr>
<td>TC votes to recommend specification</td>
<td>December 14, 2012</td>
</tr>
<tr>
<td>BoD votes to adopt specification</td>
<td>March 2013</td>
</tr>
</tbody>
</table>

### Appendix A References and Glossary Specific to this RFP

#### 6.11 A.1 References Specific to this RFP

6.12 A.2 Glossary Specific to this RFP

Accurate: Information that exactly, precisely, and correctly presents availability, usability and deploy-ability of C4ISR capability, systems and services;

Aggregation: Defines the process through which data elements are combined to referentially and semantically complete data sets.

Caveat Separation: The process for selective exchange of information based on security policy and security profiles of the information and consumer of the information. Caveat separation may apply to data elements with the information or the aggregation of information.

Communication Channel: a means of communication or access. For the purposes of this specification communication channels will be limited to the middleware used to move information between suppliers (/publishers) and consumers (/subscribers).

Confidential Information: Privileged communication shared with only a few people for furthering certain purposes, such as with an attorney for a legal matter, or with a doctor for treatment of a disease. Receiver of confidential information is generally prohibited from using it to take advantage of the supplier of that information.

Contract: A contract represents a grouping of semantics and information flow controls which specify a formal information sharing agreement between two or more operational nodes or participants in a domain or community.

Data Integrity: Compliance to the allowable types ranges or domain values for each data element (or attribute).

Data Integration: The process of combining two or more data elements from separate sources into a single semantically and referentially complete piece of information (or business object).

Domain: a sphere of knowledge or information identified by a name.

Dynamic Filters: Data and domain filters whose characteristics are set at runtime.

Challenged Networks or Communication: Under operational conditions most front line communications are provided by radio (HF, VHF, or HCDR). These forms of communications are inherently less robust than the Wi-Fi and wired
networks realized by most organizations. Challenged refers to the reality that these networks:

- Have limited bandwidth capability (as low as 1Kb/Sec);
- Are prone to outages (e.g., range limitations, jamming, and voice override);
- Large node count; and
- Packet loss.

**Classified Information:** Classified information is sensitive information to which access is restricted by law or regulation to particular classes of persons. A formal security clearance is required to handle classified documents or access classified data.

**Conceptual Interoperability:** The assumptions and constraints of the meaningful abstraction of reality – are aligned, the highest level of interoperability is reached. This requires that conceptual models are documented based on engineering methods enabling their interpretation and evaluation by other engineers.

**Common Operating Picture (COP):** A collaborative set of technologies that provide the user(s) with a shared understanding of the operational environment including: Threats; Opportunities; Resources; Situational Awareness and other relevant information. The technologies combine to integrate perspectives; deliver actionable knowledge and structure information to the specific User(s) needs.

**Common Representational Operating Picture (CROP):** Is equivalent to the COP but limits access to that information required to exercise the role or function of the user.

**Community:** a community of interest or community of practice

**Community of Interest (Col):** A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information exchanges. DoD 8320.2, December 2, 2004.

**Community of Practice:** Informal, self-organized, network of peers with diverse skills and experience in an area of practice or profession. Such groups are held together by the members' desire to help others (by sharing information) and the need to advance their own knowledge.
**Crisis Management:** Coordinated actions taken to diffuse crises, prevent their escalation into armed conflict and/or contain resulting hostilities. The crisis management machinery provides decision-makers with the necessary information and arrangements to use appropriate instruments (political, diplomatic, economic, and military) in a timely and coordinated manner. (MC 400/1).

**Data ownership:** The identification that certain parts of global (shared) information provided by all suppliers may be owned in such a way that only one entity is allowed to modify them.

**Deadline:** A QoS attribute describing the latest acceptable time for the occurrence of certain events.

**Definition:** A representation of a concept by a descriptive statement which serves to differentiate it from related concepts.

**Dynamic Interoperability:** As a system operates on data over time, the state of that system will change, and this includes the assumptions and constraints that affect its data interchange. The systems are able to identify the state changes in the assumptions and constraints and they can adjust or be adjusted to address changes in context or situation. The effect of the information exchange within the participating systems is unambiguously defined.

**Emergency Management:** The organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particularly preparedness, response and rehabilitation. *Emergency management involves plans, structures and arrangements established to engage the normal endeavours of government, voluntary and private agencies in a comprehensive and coordinated way to respond to the whole spectrum of emergency needs. This is also known as disaster management.*

**Information Artifact:** A composite of data elements that satisfy the semantics of an agreement to exchange information between a supplier and a consumer.

**Information Consumer:** Any User, System Application, Channel or Node using information managed by the IEPPS.

**Information Contract:** An agreement between an information supplier and information consumer to exchange selected information, based on a specified format, protocol and communication link.

**Information Exchange Agreement:** An agreement between an information supplier and information consumer to exchange selected information in a predefined structure.

**Information Quality:** Describes the ability of organizations, systems and persons to provide information that is:
- **Trustworthy**: information quality and content can be trusted by stakeholders, decision makers and users.

- **Relevant**: Information content tailored to specific needs of the decision maker;

- **Timely**: Information provided when and where it is needed to support the decision making process;

- **Usable**: Information is presented in a common functional format, easily understood by the decision makers and their supporting applications;

- **Complete**: Information that provides all necessary and relevant data (where available) to facilitate a decision;

- **Concise**: Information is provided in a form that is brief and succinct, yet including all important information;

- **Trusted**: Information that is accepted as authoritative by stakeholders, decision makers and users.

- **Secure**: Information is protected from inadvertent or Malicious Release to unauthorized persons, systems or organizations.

- **Protected**: Information is protected from inadvertent or malicious release

**Information Semantic (1):** A set of data elements with meaning in the sense that a computer program (or application) can learn enough about what the data means to process it

**Information Semantic (2):** A set of data elements with meaning in the sense that a consumer (e.g., user, system or application) can infer same operational equivalent to the supplier.

**Information Consumer:** This includes any user, application or system receiving information through the IES.

**Information Sharing Agreement (ISA):** an agreement between participant to share syntactically and semantically unambiguous information between members of a community.

**Information Supplier:** This includes any user, application or system providing information to the environment through the IES.

**Major Event Management** - Coordinated actions taken to plan, respond and recover from a major event such as the Olympics or State Visit. The Major Event Management machinery provides decision-makers with the necessary
information and arrangements to use appropriate instruments (political, diplomatic, economic, and military) in a timely and coordinated manner.

**Marshalling:** defines the process through which data sets are divided and put into the data elements described by the underlying data store(s)

**Messaging Protocol:** The rules, formats and functions for exchanging messages between the components of a messaging system.

**Middleware:** Software that serves as an intermediary between systems software and an application.

**Operation:** for the purpose of this RFP the term operation is restricted to events and activities describing a Crisis Response Action including Military.

**Operational Context:** a set of network, node, system, application or user characteristics that define the current state of dynamically evolving operational conditions.

**Pragmatic Interoperability:** The systems are aware of the methods and procedures that each system is using. The use of the data – or the context of its application – is understood by the participating systems; the context in which the information is exchanged is unambiguously defined. This layer puts the (word) meaning into context.

**Private Information:** Information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public.

**Proprietary Information:** Privately owned knowledge or data, such as that protected by a registered patent, copyright, or trademark.

**Real-time:** refers to the event-triggered (e.g. data change) global update of information across all nodes, systems and applications requiring access to the information.

**Static Filters:** data and information filters whose characteristics in the policy language and cannot be changed at runtime.

**QoS History:** A record of past information generated by the system that is kept around for the benefit of applications that are late joining the network.

**QoS:** Quality of Service - A set of attributes that can be used to define the middleware’s capabilities to meet the requirements of the application for the
purpose of data-delivery or management such as reliability, ownership policy, history size, time-to-keep, etc.

**Reliability:** A QoS attribute describing the guarantees and feedback provided to the application regarding the delivery of the information supplied to the middleware.

**Safeguard:** serves as protection or a guard for sensitive data or information; Designed to prevent the inadvertent of malicious release of information to unauthorized persons, systems or services; Stipulate a protection requirement or constrain on an information exchange.

**Semantic:** A semantic represents the build policy for an information composite or data composite that is specified as meaningful to participants (applications, systems and users) in a particular domain or community. Only exemplar semantics are provided in this submission as guidance to the design and development communities.

**Semantic Integrity:** Compliance to the structure, format and content (mandatory or optional) for information sets (or business objects).

**Semantic Interoperability:** a common information exchange reference model is used. The meaning of the data is shared; the content of the information exchange requests are unambiguously defined. This layer defines (word) meaning.

**Syntactic Interoperability:** a common structure to exchange information; i.e., a common data format is applied. On this level, a common protocol to structure the data is used; the format of the information exchange is unambiguously defined.

**Stage:** to gather and prepare information for release to a community in accordance with established policy, memorandum of understanding or service level agreements.

**Tearline:** A logical line in a message or document separating categories of information that have been approved for disclosure and release.

**Technical Interoperability:** An agreed communication protocol exists for exchanging data between participating systems. The protocol operates over an agreed and established communication infrastructure allowing systems to exchange bits and bytes, and the underlying networks and protocols are unambiguously defined.
Transactional: A Transactional represent the build policy for a reusable information building blocks, often realized as business objects comprising the community logical data model, for which there is likely also an underlying information or data store; they maintain the referential and data integrity of that store. Transactionals form the core of this specification.

Transformation: The conversion of data and information elements from a source data format/syntax/structure into destination data format/syntax/structure

Trusted Information Exchange: The ability to selectively control the dissemination of information from an information supplier to an information consumer based on operational context; supplier and consumer capability; network QoS; and adhering to operating, security, network, etc., policies established for the operation.

Trust: Within the scope of this RFP – Trust refers to the level of confidence an information supplier has relating to the release of selected information to a specific consumer of that information.

Vocabulary: A representation of a set of concepts by formal, descriptive statements which serves to differentiate those concepts from related concepts within a given domain or area of expertise.

6.13 A.3 Acronyms Specific to this RFP

C4I Command, Control, Communications, Collaboration and Intelligence

COP Common Operational Picture

CRO Crisis Response Operation

CROP Common Representative Operational Picture

DEM Data Exchange Mechanism

DHS Department of Homeland Security

DTF Domain Task Force

FICAM Federal ICAM

HCDR High Capacity Digital Radio
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>HF</td>
<td>High Frequency</td>
</tr>
<tr>
<td>ICAM</td>
<td>Identity, Credentials and Access Management</td>
</tr>
<tr>
<td>IEA</td>
<td>Information Exchange Agreement</td>
</tr>
<tr>
<td>IEDM</td>
<td>Information Exchange Data Model</td>
</tr>
<tr>
<td>IEF</td>
<td>Information Exchange Framework</td>
</tr>
<tr>
<td>IEP</td>
<td>Information Exchange Policy</td>
</tr>
<tr>
<td>IEPPS</td>
<td>Information Exchange Policy-based Packaging Service</td>
</tr>
<tr>
<td>IEPMS</td>
<td>Information Exchange Policy Management Service</td>
</tr>
<tr>
<td>IEPV</td>
<td>Information Exchange Policy Vocabulary</td>
</tr>
<tr>
<td>IEPL</td>
<td>Information Exchange Policy Language</td>
</tr>
<tr>
<td>IES</td>
<td>Information Exchange Mechanism</td>
</tr>
<tr>
<td>ISA</td>
<td>Information System Application</td>
</tr>
<tr>
<td>ISE</td>
<td>Information Sharing Environment</td>
</tr>
<tr>
<td>MDA</td>
<td>Model Driven Architecture</td>
</tr>
<tr>
<td>MEM</td>
<td>Message Exchange Mechanism</td>
</tr>
<tr>
<td>MIP</td>
<td>Multilateral Interoperability Programme</td>
</tr>
<tr>
<td>MLS</td>
<td>Multi-level Security</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Government Organization</td>
</tr>
<tr>
<td>OODBMS</td>
<td>Object Oriented Database Management System</td>
</tr>
<tr>
<td>ORDBMS</td>
<td>Object-Relational Database Management System</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PIM</td>
<td>Platform Independent Model</td>
</tr>
<tr>
<td>PM-ISE</td>
<td>Project Manager Information Sharing Environment</td>
</tr>
</tbody>
</table>
6.14 Appendix B General Reference and Glossary

6.15 B.1 General References

The following documents are referenced in this document:

[ATC] Air Traffic Control Specification,  
http://www.omg.org/technology/documents/formal/air_traffic_control.htm

[BCQ] OMG Board of Directors Business Committee Questionnaire,  
http://doc.omg.org/bc/07-08-06


[CCM] CORBA Core Components Specification,  

[CORBA] Common Object Request Broker Architecture (CORBA/IIOP),  

[CSIV2] [CORBA] Chapter 26

[CWM] Common Warehouse Metamodel Specification,  
[DAIS] Data Acquisition from Industrial Systems,
http://www.omg.org/technology/documents/formal/dais.htm


[EDOC] UML Profile for EDOC Specification,
http://www.omg.org/techprocess/meetings/schedule/UML_Profile_for_EDOC_FTF.html

[EJB] “Enterprise JavaBeans™”,

[FORMS] “ISO PAS Compatible Submission Template”.
http://www.omg.org/cgi-bin/doc?pas/2003-08-02

[GE] Gene Expression,

[GLS] General Ledger Specification ,


[IDL] ISO/IEC 14750 also see [CORBA] Chapter 3.

[IDLC++] IDL to C++ Language Mapping,

[JAAS] Java™ Authentication and Authorization Service;
http://download.oracle.com/javase/6/docs/technotes/guides/security/jaas/JAASRefGuide.html

[JCA] Java™ Cryptography Architecture JCA.

National Information Exchange Model Information Exchange Package Description (IEPD); https://www.niem.gov/fordomains/Pages/for-domains.aspx

[Inventory] Inventory of Files for a Submission/Revision/Finalization, http://doc.omg.org/smsc/2007-09-05

[LEXS] Logical Entity eXchange Specification 4.0 http://130.207.211.107/content/lexs-overview


6.16 B.2 General Glossary

**Architecture Board (AB)** - The OMG plenary that is responsible for ensuring the technical merit and MDA-compliance of RFPs and their submissions.

**Board of Directors (BoD)** - The OMG body that is responsible for adopting technology.

**Common Object Request Broker Architecture (CORBA)** - An OMG distributed computing platform specification that is independent of implementation languages.

[RM-ODP] ISO/IEC 10746


**Common Warehouse Metamodel (CWM)** - An OMG specification for data repository integration.

**CORBA Component Model (CCM)** - An OMG specification for an implementation language independent distributed component model.

**Interface Definition Language (IDL)** - An OMG and ISO standard language for specifying interfaces and associated data structures.

**Letter of Intent (LOI)** - A letter submitted to the OMG BoD’s Business Committee signed by an officer of an organization signifying its intent to respond to the RFP and confirming the organization’s willingness to comply with OMG’s terms and conditions, and commercial availability requirements.

**Mapping** - Specification of a mechanism for transforming the elements of a model conforming to a particular metamodel into elements of another model that conforms to another (possibly the same) metamodel.

**Metadata** - Data that represents models. For example, a UML model; a CORBA object model expressed in IDL; and a relational database schema expressed using CWM.

**Metamodel** - A model of models.

**Meta Object Facility (MOF)** - An OMG standard, closely related to UML, that enables metadata management and language definition.

**Model** - A formal specification of the function, structure and/or behavior of an application or system.

**Model Driven Architecture (MDA)** - An approach to IT system specification that separates the specification of functionality from the specification of the implementation of that functionality on a specific technology platform.

**Normative** – Provisions that one must conform to in order to claim compliance with the standard. (as opposed to non-normative or informative which is explanatory material that is included in order to assist in understanding the standard and does not contain any provisions that must be conformed to in order to claim compliance).

**Normative Reference** – References that contain provisions that one must conform to in order to claim compliance with the standard that contains said normative reference.
**Platform** - A set of subsystems/technologies that provide a coherent set of functionality through interfaces and specified usage patterns that any subsystem that depends on the platform can use without concern for the details of how the functionality provided by the platform is implemented.

**Platform Independent Model (PIM)** - A model of a subsystem that contains no information specific to the platform, or the technology that is used to realize it.

**Platform Specific Model (PSM)** - A model of a subsystem that includes information about the specific technology that is used in the realization of it on a specific platform, and hence possibly contains elements that are specific to the platform.

**Request for Information (RFI)** - A general request to industry, academia, and any other interested parties to submit information about a particular technology area to one of the OMG's Technology Committee subgroups.

**Request for Proposal (RFP)** - A document requesting OMG members to submit proposals to an OMG Technology Committee. Such proposals must be received by a certain deadline and are evaluated by the issuing Task Force.

**Task Force (TF)** - The OMG Technology Committee subgroup responsible for issuing a RFP and evaluating submission(s).

**Technology Committee (TC)** - The body responsible for recommending technologies for adoption to the BoD. There are two TCs in OMG – the Platform TC (PTC) focuses on IT and modeling infrastructure related standards; while the Domain TC (DTC) focuses on domain specific standards.

**Unified Modeling Language (UML)** - An OMG standard language for specifying the structure and behavior of systems. The standard defines an abstract syntax and a graphical concrete syntax.

**UML Profile** - A standardized set of extensions and constraints that tailors UML to particular use.

**XML Metadata Interchange (XMI)** - An OMG standard that facilitates interchange of models via XML documents.