Object Management Group

140 Kendrick Street
Building A Suite 300
Needham, MA 02494
USA

Telephone: +1-781-444-0404
Facsimile: +1-781-444-0320

Information Exchange Framework

Information Exchange Policy Vocabulary

(IEPV)

Request For Proposal

OMG Document: mars/2011-03-15

Letters of Intent due: 18 June 2011

Submissions due: 14 November 2011

Objective of this RFP

The objective of Information Exchange Framework (IEF) Policy Vocabulary is to enhance the ability of organizations to describe the rules governing the sharing and protection of information. The IEF Information Exchange Policy Vocabulary RFP seeks to provide a robust vocabulary for expressing the policies, rules and constraints governing the release and exchange of information between information systems participating in an information sharing agreement. This specification will provide a formal vocabulary that is able to express the

nouns and verbs used to construct statements that can be encoded as a set of human and machine readable policies and then enforced by software applications and services.

This RFP solicits proposals for a formal vocabulary that can be expressed in one or more software enforceable policy languages. Submissions should specify how these policies are sufficient to permit rigorous modeling, validation and enforcement.

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 actually represented on a storage medium based on some particular data storage paradigm etc., and a mapping from the PIM to each PSM.

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.

For more detailed information on the adoption process see the *Policies and Procedures of the OMG Technical Process* [P&P] and the *OMG Hitchhiker's*

Guide [Guide]. In case of any inconsistency between this document and the [P&P] in all cases the [P&P] shall prevail.

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

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.

A2 Business Committee evaluation criteria

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.

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.

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.

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.

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.

4.5 Responding to RFP items

4.5.1 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.

4.5.2 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.

4.5.3 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.

4.6 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.

4.7 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.

4.8 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.

4.9 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.

4.9.1 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].

4.9.2 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.

4.10 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

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: first: 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 increasing 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 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 Ontology PSIG and 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 Request for Proposal represents the first in a series of IEF related RFPs, to be released by MARS. The three proposed IEF RFPs include Policy Vocabulary, Policy Manager, and Policy Enforcement Service. **Error! Reference source not found.** Figure 6-1 provides the contextual relationships between the IEF RFPs and other participating elements in the eco-system.

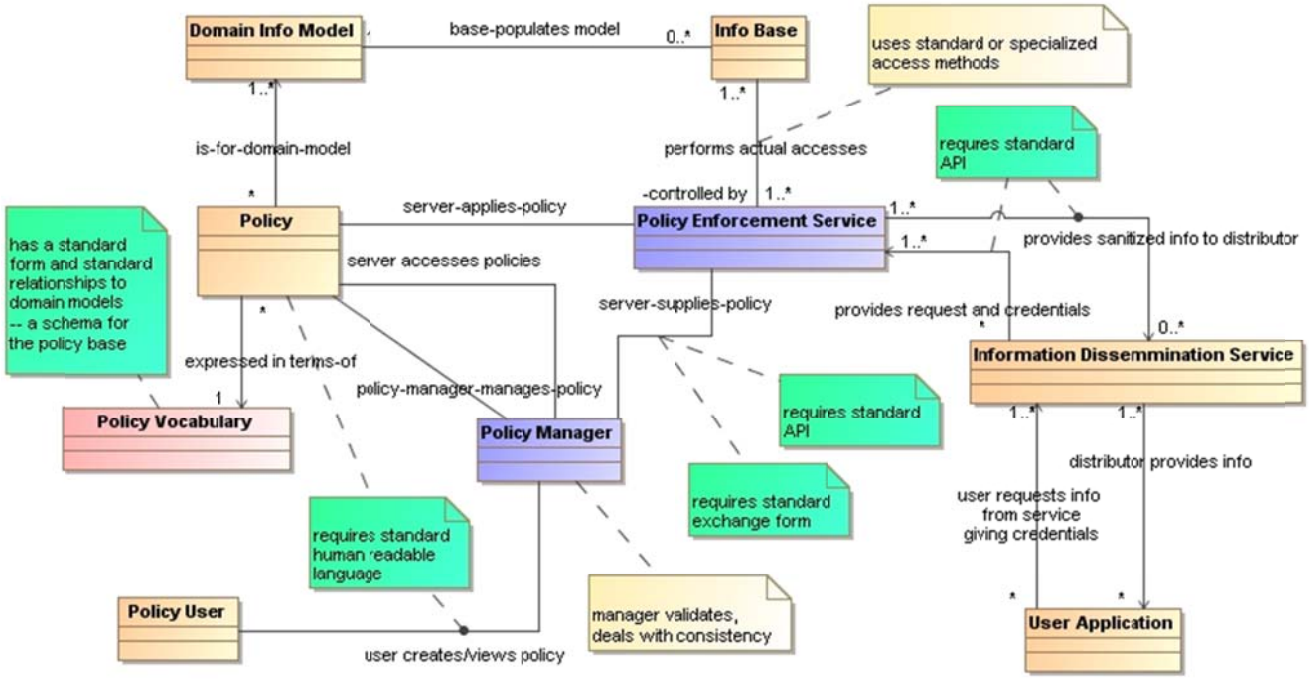

Figure 6-1 – IEF Policy Vocabulary and Rule Specification

The overall objective of the IEF is to use policies (expressed using a standard vocabulary) to control the Information Exchange Policy Enforcement Services (IEPES), one of two IEF specifications to be issued at a later date. The IEPES will enforce the policies that

govern an information sharing agreement. It will incorporate, integrate, and/or interoperate with capabilities including, but not limited to:

- Middleware (e.g., SOA, Web Services, DDS and CORBA)
- Event logging Services;
- Security Services;
- User Defined Services;
- Auditing Services;
- Certification Services;
- Policy Management Services

This RFP solicits proposals for a vocabulary specification for policy concepts for the release of information, including the rules and characteristics that govern its exchange. Proposals should explain not only the relevant vocabulary but show how the vocabulary can be used to model and validate information sharing policies (in the context of this RFP , "validated" means that one should be able to use/build tools that, for example, will determine whether or not the policies expressed in the vocabulary are logically consistent, and whether or not there are any unsatisfiable conditions expressed in the policy statements.) The resulting vocabulary must be expressible in terms of policy languages that support both human and machine-readable form(s).

6.2.1 Semantic Interoperability

The goal of this RFP is to define a standardized vocabulary for specifying user policies (semantics, rules and constraints) that govern the release of information across system and organizational boundaries. The ability to specify these policies is not necessarily system, application or technology specific; however, such a capability is not well supported by existing enterprise and system architecture frameworks. The lack of uniform architectural practices and a common vocabulary for specifying and detailing these critical requirements, coupled with an expanding need to balance the conflicting requirements to share and, at the same time, protect information assets, is becoming the central challenge for Information Management. Systems are increasingly more difficult and costly to certify, accredit, and maintain in environments where sensitive (private, confidential, classified and/or legally sensitive) information is required to achieve desired outcomes.

Semantic interoperability refers to the capacity of information systems to exchange information in such a manner that information is properly and consistently interpreted by the receiving system; in other words, the interpretation of a receiving system must be the same interpretation as intended by the sending system. Semantic interoperability requires that two or more systems derive the same interpretations from the same information. This implies that the developers and users of the systems can specify the rules for exchange over each interface in a clear, concise and unambiguous manner. For this to occur, users, analyst, architects, engineers and developers need a common vocabulary to express and communicate these rules.

This vocabulary must be precise enough to support machine reasoning to drive data aggregation, transformation, filtering and machine to machine interoperability. In addition, one should be able to use/build tools that, for example, will determine whether or not the policies expressed in the vocabulary are logically consistent, and whether or not there are any unsatisfiable conditions expressed in the policy statements.

6.3 Relationship to Existing OMG Specifications

The intent is for submissions to maximize the use of existing and evolving OMG standards in at least one Platform Specific Model and implementation. We are not specifying these relationships; however, submitters are encouraged to use related internationally or commercially accepted standards that deliver all or part of the requested capability.

OMG Standards that should be considered include[1]:

- Unified Profile for DODAF and MODAF (UPDM).
- Shared Operational Picture Exchange Services (SOPES) Information Exchange Data Model (IEDM), Information Management Metamodel (IMM), and Query View Transformation (QVT): specifications that describe patterns related to data and model transformation and integration.
- Data Distribution for Real-time Systems (DDS) and Common Object Request Broker Architecture (CORBA): information exchange mechanism specifications whose configuration should be describable by the vocabulary.
- Model Driven Message Interoperability (MDMI): may be considered for the development of vocabularies.
- Ontology Definition Metamodel (ODM): a specification for ontology and vocabulary specifications.
- Semantics of Business Vocabulary and Rules (SBVR): a specification for expressing vocabularies and rules.
- Unified Modeling Language (UML), Service Oriented Architecture Modeling Language (SoaML): specifications that provide capabilities for expressing vocabularies and rules.
- XML Metadata Interchange (XMI): a specification for the exchange of the vocabularies.

The submitters are free to reference additional standards and publically accepted specifications as part of their submissions.

[1] References to these specifications and standards are provided in Annex B.1.

6.4 Related 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.

Because the IEF effort is generally targeting the C4I, Public Safety and Security, and Emergency Management domains, there is particular interest in supporting a number of community-derived Extensible Mark-up Language (*XML*) based exchange standards/specifications, such as those identified below:

- National Information Exchange Model (NIEM)
- Emergency Management Information Standards
    1. Common Alerting Protocol (CAP)
    2. Emergency Data Exchange Language - Distribution Element (EDXL-DE)
    3. Emergency Data Exchange Language - Resource Messaging (EDXL-RM)
    4. Emergency Data Exchange Language - Hospital Availability Exchange (EDXL-HAVE)
    5. Cyclone Warning Markup Language (CWML)
    6. Tsunami Warning Markup Language (TWML)
    7. People Finder Interchange Format PFIF
    8. Tactical Situation Object TSO
- Geospatial Standards:
    1. GeoRSS
    2. Geography Markup Language (GML)
    3. Web Feature Service (WFS)
    4. Web Mapping Service (WMS)
    5. Sensor Observation Service (SOS)
    6. SensorML
    7. Sensor Planning Service (SPS)
- Consultation, Command and Control (Military Interface)
    1. Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM)
    2. Multilateral Interoperability Program (MIP) XML
    3. Universal CORE (UCORE)

4. C2 CORE

- Healthcare (HL7 (Emergency Response and Public Health))

In addition to these community vocabulary specifications, submitters should use, where applicable, standardized policy languages as part of their Platform Specific Models, such as:[2]

- OASIS SOA Reference Model
- Security Assertion Markup Language 2.0 (*SAML* 2.0)
- eXtensible Access Control Markup Language (XACML 1.0)
- Business Process Execution Language (BPEL)
- Ponder
- Simple Knowledge Organization System (SKOS)
- ISO 11179-3 Edition 3
- Common Terminology Services 2 (CTS2)

This 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.
Note: Although the IEF is targeting specific communities, the submitters should avoid using domain specific vocabularies and focus on a domain independent vocabulary that is extendable to other information domains and platforms.

6.5 Mandatory Requirements

1. The submission shall define a formal vocabulary that allows polices about information exchange to be expressed in a consistent, unambiguous manner. By this we mean that the vocabulary shall consist of terms and formal definitions that are logically consistent and sufficient to support rule development and/or machine reasoning.

2. The vocabulary shall be expressed in a formal vocabulary expression language, such as SBVR, or OWL, or MOF/OCL.

3. The submission shall identify at least one policy or transformation language in use that illustrates that the vocabulary is expressible (e.g. Ponder, SBVR, and SAML). Examples shall be provided that show the relationship between the vocabulary elements and the language elements.

4. The vocabulary specified in the submission shall enable users to express the characteristics of the information channel, session or interface required to transfer or exchange the information, including but not limited to:

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

a. The allowable participants to the exchange (e.g., Publishers/Senders and Subscribers/ Receivers).

b. The message protocols to be applied to the exchange.

c. The network protocols to be applied to the exchange.

d. The quality of service (QOS) characteristics for the exchange.

e. The network and communication safeguards to be applied to the exchange.

5. The vocabulary specified in the submission shall enable users to express the rules and constraints governing the processing of the information and data elements by the IEPES, including:

a. The information patterns that define how information and data elements are combined at runtime to form the community semantics for exchange.

b. The mandatory and optional inclusion of data and information elements in an aggregate.

c. The specialization patterns depending on characteristics (e.g., category codes) contained in the instance data.

d. The relationships between element names that differ in physical, logical and conceptual representations.

e. The static, unchangeable at runtime, filtering for data and information elements during aggregation of instance data.

f. The dynamic filtering of data and information elements, set at runtime, during the aggregation of instance data.

g. The transformation of data attributes and domains to satisfy organization and community semantics;

h. The labeling of information elements aggregates vis-à-vis the labels associated with the underlying data elements.

6. The vocabulary specified in the submission shall enable users to express the rules governing the protection and release-ability of information on selected middleware, network and/or communication channels.

7. The submission shall describe the Terminology used for expressing the aggregation and transformation of data and information elements to conform to community agreed policies and semantics.

6.6 Optional Requirements

1. The expression of other policy, rules and constraints which assure that information is Accurate, Relevant, Timely, Usable, Complete, Concise, Trusted, and Secure.

6.7 Issues to be discussed

1. ODM/OWL as a basis for specifying and validating the vocabulary.

2. Use of the vocabulary in conjunction with an existing policy language (e.g., WSPL, WSS, SPL, AIR, Ponder)[3].

3. Relationship to standards that may have contributed to this submission (e.g., UPDM, SOPES, CORBA, DDS, MOF, ODM, QVT, SBVR and IMM).

4. Addressing the flexibility, extensibility, supportability and maintainability of the submitted policy vocabulary.

5. How the vocabulary can be applied to Architecture, Architecture Frameworks and MDA.

6. How the vocabulary can be used to create information exchange policies, how these policies can be modeled, and how these policy models can be validated.

7. How tool vendors will apply the vocabulary to system and software platforms.

8. How the vocabulary can be applied to existing standards and specifications (e.g., SOPES IEDM and NIEM).

6.8 Evaluation Criteria

More desirable submissions are those that:

1. Meet high levels of compliance as defined in sections 6.5 and 6.6 including:
    a. Completeness of the Policy Vocabulary.
    b. Ability to describe configuration of exchange mechanisms such as CORBA, DDS, MIP DEM, SOA, Web Services and other commercial data-centric middleware.
    c. Flexibility, extensibility, maintainability, supportability and ease of use.
    d. Levels of information protection and information security provided.

2. Alignment with Architecture, Architecture Frameworks and MDA, including:
    a. Ease of implementation on a variety of systems and software platforms.
    b. Incorporation/integration of existing standards and specifications (e.g., SOPES IEDM).

3. Demonstrate the availability of one or more language implementations.

[3] References to these specifications and standards can be found in Annex B.2.

6.9 Other information unique to this RFP

Not Applicable.

6.10 RFP Timetable

The timetable for this RFP is given below. Note that the TF or its parent TC may, in certain circumstances, extend deadlines while the RFP is running, or may elect to have more than one Revised Submission step. The latest timetable can always be found at the OMG *Work In Progress* page at http://www.omg.org/schedules/ under the item identified by the name of this RFP. Note that "<month>" and "<approximate month>" is the name of the month spelled out; e.g., January.

Event or Activity	Actual Date
Preparation of RFP by TF	
RFP placed on OMG document server	*21 Feb 2011*
Approval of RFP by Architecture Board *Review by TC*	*24 Mar 2011*
TC votes to issue RFP	*25 Mar 2011*
LOI to submit to RFP due	*18 June 2011*
Initial Submission presentations by submitters	*12 December 2011*
Initial Submissions due and placed on OMG document server ("Four week rule")	*14 November 2011*
Voter registration closes	*15 December 2011*
Initial Submission presentations	*12 December 2011*
Preliminary evaluation by TF	*December 2011*
Revised Submissions due and placed on OMG document server ("Four week rule")	*21 May 2012*
Revised Submission presentations	*18 June 2012*
Final evaluation and selection by TF *Recommendation to AB and TC*	*10 September 2012*
Approval by Architecture Board *Review by TC*	*13 September 2012*
BoD votes to adopt specification	*20 September 2012*

7.0 Appendix A References and Glossary Specific to this RFP

7.1 A.1 References Specific to this RFP

For reference, Multilateral Interoperability Programme Specification can be found at http://www.mip-site.org/.

7.2 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.

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).

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.

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 of Interest (CoI): "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.

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.

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 IES.

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 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)

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.

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

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.

7.3 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
DTF	Domain Task Force
HCDR	High Capacity Digital Radio
HF	High Frequency
IEA	Information Exchange Agreement
IEDM	Information Exchange Data Model
IEPES	Information Exchange Policy Enforcement Service
IEPMS	Information Exchange Policy Management Service
IEPL	Information Exchange Policy Vocabulary
IES	Information Exchange Mechanism
ISA	Information System Application
MDA	Model Driven Architecture
MEM	Message Exchange Mechanism
MIP	Multilateral Interoperability Programme
MLS	Multi-level Security
NGO	Non-Government Organization
OODBMS	Object Oriented Database Management System
ORDBMS	Object-Relational Database Management System
PDU	Protocol Data Unit
PIM	Platform Independent Model
PSM	Platform Specific Model

PVO	Private Volunteer Organization
QoS	Quality of Service
QOS	Quality of Service
RDBMS	Relational Database Management System
SA	Situational Awareness
SOPES	Shared Operational Picture Exchange Services
TER	Transmission Efficiency Rules
TIE	Trusted Information Exchange
VHF	Very High Frequency

Appendix B General Reference and Glossary

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, *http://www.omg.org/technology/documents/formal/components.htm*

[CORBA] Common Object Request Broker Architecture (CORBA/IIOP), *http://www.omg.org/technology/documents/formal/corba_iiop.htm*

[CSIV2] [CORBA] Chapter 26

[CWM] Common Warehouse Metamodel Specification, *http://www.omg.org/technology/documents/formal/cwm.htm*

[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™”, *http://java.sun.com/products/ejb/docs.html*

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

[GE] Gene Expression,
http://www.omg.org/technology/documents/formal/gene_expression.htm

[GLS] General Ledger Specification ,
http://www.omg.org/technology/documents/formal/gen_ledger.htm

[Guide] The OMG Hitchhiker's Guide,, *http://www.omg.org/cgi-bin/doc?hh*

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

[IDLC++] IDL to C++ Language Mapping,
http://www.omg.org/technology/documents/formal/c++.htm

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

[MDAa] OMG Architecture Board, "Model Driven Architecture - A Technical Perspective", *http://www.omg.org/mda/papers.htm*

[MDAb] "Developing in OMG's Model Driven Architecture (MDA),"
http://www.omg.org/docs/omg/01-12-01.pdf

[MDAc] "MDA Guide" (*http://www.omg.org/docs/omg/03-06-01.pdf*)

[MDAd] "MDA "The Architecture of Choice for a Changing World™"",
http://www.omg.org/mda

[MOF] Meta Object Facility Specification,
http://www.omg.org/technology/documents/formal/mof.htm

[MQS] "MQSeries Primer",
http://www.redbooks.ibm.com/redpapers/pdfs/redp0021.pdf

[NS] Naming Service,
http://www.omg.org/technology/documents/formal/naming_service.htm

[OMA] "Object Management Architecture™", *http://www.omg.org/oma/*

[OTS] Transaction Service,
http://www.omg.org/technology/documents/formal/transaction_service.htm

[P&P] Policies and Procedures of the OMG Technical Process,
http://www.omg.org/cgi-bin/doc?pp

[PIDS] Personal Identification Service,
http://www.omg.org/technology/documents/formal/person_identification_service.htm

[RAD] Resource Access Decision Facility,
http://www.omg.org/technology/documents/formal/resource_access_decision.htm

[RFC2119] IETF Best Practices: Key words for use in RFCs to Indicate Requirement Levels, (*http://www.ietf.org/rfc/rfc2119.txt*).

[RM-ODP] ISO/IEC 10746

[SEC] CORBA Security Service, *http://www.omg.org/technology/documents/formal/security_service.htm*

[TOS] Trading Object Service, *http://www.omg.org/technology/documents/formal/trading_object_service.htm*

[UML] Unified Modeling Language Specification, *http://www.omg.org/technology/documents/formal/uml.htm*

[UMLC] UML Profile for CORBA, *http://www.omg.org/technology/documents/formal/profile_corba.htm*

[XMI] XML Metadata Interchange Specification, *http://www.omg.org/technology/documents/formal/xmi.htm*

[XML/Value] XML Value Type Specification, *http://www.omg.org/technology/documents/formal/xmlvalue.htm*

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.

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.