Open GIS Consortium Inc.

Date: 2003-05-19

Reference number of this Open GIS© Project Document: **OGC 03-061**

Version: 0.7.0

Category: Open GIS© OGC Interoperability Program Report –Viewpoint Specification

Editor: Geoffrey Ehler (Lockheed Martin)

Critical Infrastructure Collaborative Environment Architecture:

Enterprise Viewpoint

Warning

This document is not an OGC Standard or Specification. This document presents a discussion of technology issues considered in an Interoperability Initiative of the OGC Interoperability Program. The content of this document is presented to create discussion in the geospatial information industry on this topic; the content of this document is not to be considered an adopted specification of any kind. This document does not represent the official position of the OGC nor of the OGC Technical Committee. It is subject to change without notice and may not be referred to as an OGC Standard or Specification. However, the discussions in this document could very well lead to the definition of an OGC Implementation Specification.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type:	Open GIS© Draft Interoperability Program Report –Viewpoint Specification
Document subtype:	OGC Critical Infrastructure Protection Initiative (CIPI)
Document stage:	Draft
Document language:	English

Contents

i. Preface

The Open GIS Consortium (OGC) is an international industry consortium of more than 250 companies, government agencies, and universities participating in a consensus process to develop publicly available geo-processing specifications. This Draft Interoperability Program Report (DIPR) is a product of the OGC Critical Infrastructure Protection Initiative (CIPI), the objective of which is to provide a vendor-neutral interoperable framework that enables collaborating communities to rapidly and collaboratively publish, discover, integrate and use geospatial information concerned with the protection of critical infrastructure systems in a range of sectors. Specifically, this document specifies an Enterprise Architecture viewpoint for a Critical Infrastructure Collaborative Environment (CICE).

The OGC Critical Infrastructure Protection Initiative is part of the OGC's Interoperability Program: a global, collaborative, hands-on engineering and testing program designed to deliver prototype technologies and proven candidate specifications into the OGC's Specification Development Program. In OGC Interoperability Initiatives, international teams of technology providers work together to solve specific geo-processing interoperability problems posed by Initiative sponsors.

We note that while this document focuses initially on critical infrastructure protection in the United States and Canada, the Enterprise descriptions herein are positioned to address the CIP needs of other nations around the globe. To assist in broadening the scope of examples used to describe the CICE, the authors of this document invite contributions from other national government representatives. Please refer your contributions to the Points of Contact listed in section ii of this document.

ii. Document Contributor Contact Points

All questions regarding this document should be directed to the editor or the contributors:

Geoffrey Ehler
Lockheed Martin
geoffrey.b.ehler@lmco.com

John Moeller
Northrup Grumman IT/TASC
jmoeller@northropgrumman.com

iii. Revision History

Date	Release	Description
2003-01-16	0.1.0	▪ Template populated with the preliminary table of contents; ▪ Refined scope; ▪ Added reference material; ▪ Added Moeller draft material.
2003-02-27	0.2.0	▪ Document revisions, Moeller, Ehler.
2003-03-07	0.3.0	▪ Document revisions, Moeller, Ehler.
2003-03-16	0.4.0	▪ Document revisions, Moeller, Ehler.
2003-05-07	0.5.0	▪ Document revisions, Moeller, Ehler.
2003-05-12	0.6.0	▪ Ehler incorporated revisions from Jeff Simon, Mark Reichardt.
2003-05-19	0.7.0	▪ Ehler added document number.

.

1 Introduction

This candidate specification addresses the Enterprise architecture viewpoint for a system dedicated to the protection of critical infrastructure components -- it is concerned with the describing the purpose, scope, and policies of a system. ISO Reference Model for Open Distributed Processing (RM-ODP) (ISO/IEC 10746) is the framework adopted by the OGC for specifying its reference architectures. The four main parts of the RM-ODP framework define viewpoints on open distributed processing (ODP) systems.

1.1 Document Scope

This Draft Interoperability Program Report (DIPR) specifies the Enterprise viewpoint for the Critical Infrastructure Collaborative Environment (CICE). This open, distributed processing environment crosses organizational boundaries and includes a variety of components deployed within multiple communities. The CICE leverages OGC Web Services to enable:

- The publication of the availability of critical infrastructure services and data;
- The registration and categorization of published service and data providers; and
- The discovery of needed critical infrastructure services and data
- The integration and application of critical infrastructure services and data

Critical infrastructure is a very broad term that encompasses many large-scale systems in a range of sectors: energy, telecommunications, transportation, public health services, and more. Safeguarding such systems involves a myriad of political, economic, and legal issues that will not be raised here. Rather, the CICE is more about the creation and maintenance of a *common information operating environment* to support operational, planning, and decision-making activities associated with critical infrastructure protection.

1.2 Conformance

Assessing conformance requires consistency across the various viewpoints (i.e., clear mappings of concepts) and across the models they define. In general, the set of viewpoint specifications should not make mutually contradictory statements. Furthermore, each specification should include correspondence statements that relate it to other viewpoints.

1.3 Normative references

The following normative documents contain provisions, which, through reference in this text, constitute provisions of this Interoperability Program Report. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this document are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

ISO/IEC 10746-2:1996, *Information Technology – Open Distributed Processing –Reference Model: Foundations*.

ISO/IEC 10746-3:1996, *Information Technology – Open Distributed Processing –Reference Model: Architecture.*

ISO/IEC 15414:2001, *Information Technology – Open Distributed Processing –Enterprise Language.*

ISO/IEC 15935:1998, *Information Technology – Open Distributed Processing – Reference Model: Quality of Service.*

OGC 02-077:2002, *Open GIS Reference Model.*

1.4 Terms and definitions

For the purposes of this Draft Interoperability Program Report, the terms and definitions given in ISO 10746-2 and ISO 10746-3 apply. For convenience, some of these terms are repeated below.

1.4.1 Critical infrastructure

Critical infrastructure, as defined by the "U.S. Patriot Act", are described as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

1.4.2 Policy

A set of obligation, prohibition, or permission rules that either constrain or enable actions, as related to a purpose. [ISO 10746-2]

1.5 Conventions

1.5.1 Symbols and abbreviated terms

The following symbols and abbreviated terms are used in this document.

ANSI	American National Standards Institute
BRM	Business Reference Model
CI	Critical infrastructure
CICE	Critical Infrastructure Collaborative Environment
CIP	Critical Infrastructure Protection
CIPI	Critical Infrastructure Protection Initiative

DIPR	Draft Interoperability Program Report
FEA	Federal Enterprise Architecture
FGDC	Federal Geographic Data Committee
GIRM	Geospatial Interoperability Reference Model
GSDI	Global Spatial Data Infrastructure
ISO	International Organization for Standardization
NSDI	National Spatial Data Infrastructure
ODP	Open Distributed Processing
OGC	Open GIS Consortium
ORM	Open GIS Reference Model
QoS	Quality of Service
RM-ODP	Reference Model for Open Distributed Processing
SDI	Spatial Data Infrastructure

2 The CICE Architecture

The Critical Infrastructure Collaborative Environment (CICE) Architecture is a component of the OGC Reference Model, which is a living document that describes the architectural construct for the Open GIS Consortium's geoprocessing interoperability specifications. The CICE performs two roles in relation to the OGC Reference Model (ORM). First, it is guided by the principals and established procedures of the ORM. Second, it represents a key area of activity that develops and defines the ORM. Through activities and initiatives such as CICE, the ORM is developed, and improved.

2.1 Relationship to OGC and Other Architectures

The CICE also contributes to other architectures through the ORM. In the United States, the ORM contributes significantly to the National Spatial Data Infrastructure, and is characterized in the Geospatial Interoperability Reference Model (GIRM) being developed by the Federal Geographic Data Committee. The GIRM is intended to be a document that will guide Federal Agencies in using reusable elements that are built on standards from ISO, ANSI, OGC and other consensus standards bodies (Figure 1). The GIRM additionally will be used in the United States to facilitate the inclusion of Geospatial architectural elements into its Federal Enterprise Architecture (Figure 2). Indeed, the ORM offers a core interoperability reference for NSDI architectures around the globe including the Australian Spatial Data Infrastructure, the Canadian Geospatial Data Infrastructure (CGDI), and many others.

The Relationship Between International and U.S. National Standardization Initiatives

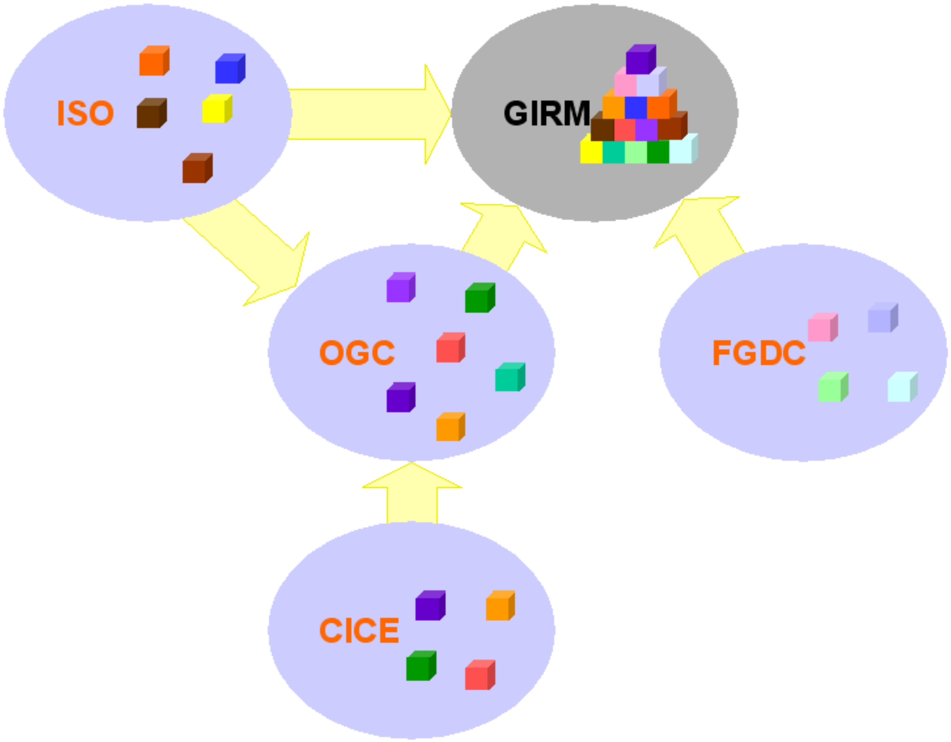
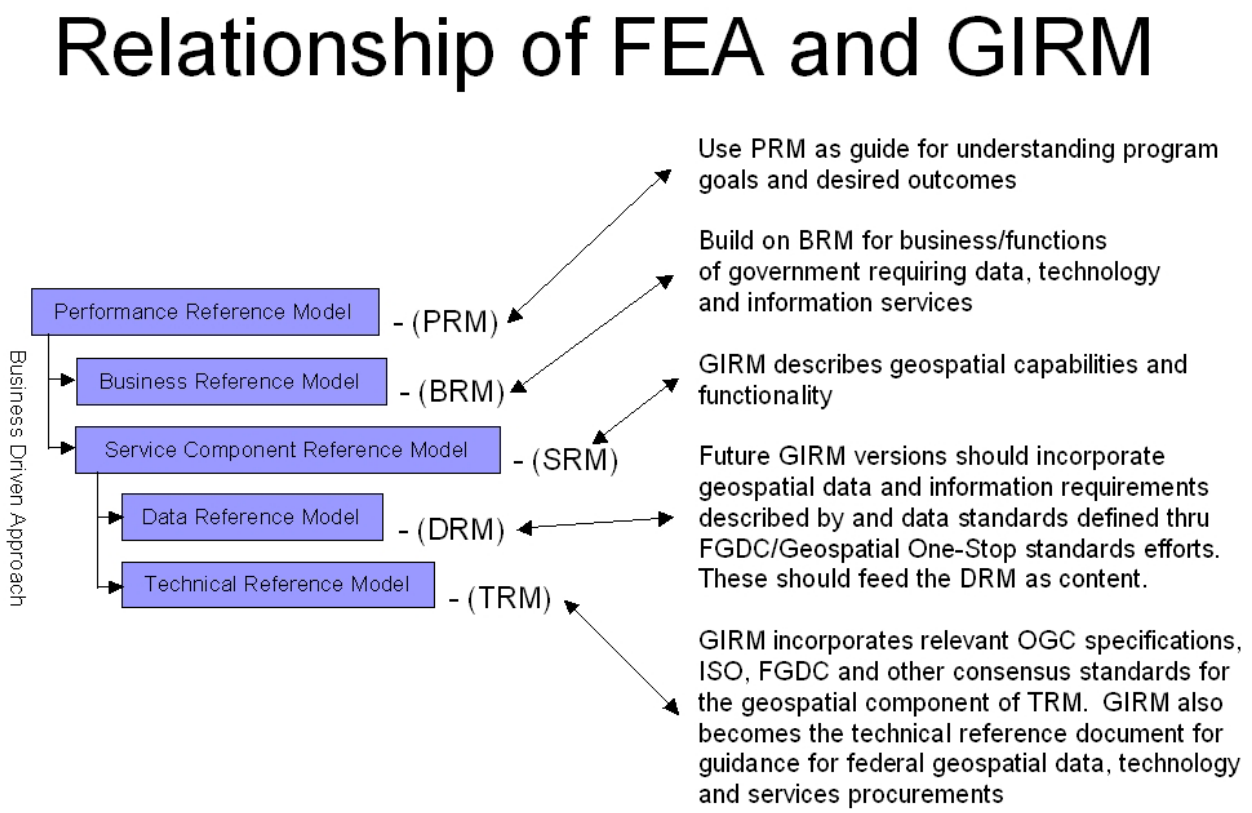


Figure 1. The CICE Enterprise Architecture Supports OGC and U.S. Architecture Initiatives.



Relationship of FEA and GIRM

Use PRM as guide for understanding program goals and desired outcomes

Build on BRM for business/functions of government requiring data, technology and information services

GIRM describes geospatial capabilities and functionality

Future GIRM versions should incorporate geospatial data and information requirements described by and data standards defined thru FGDC/Geospatial One-Stop standards efforts. These should feed the DRM as content.

GIRM incorporates relevant OGC specifications, ISO, FGDC and other consensus standards for the geospatial component of TRM. GIRM also becomes the technical reference document for guidance for federal geospatial data, technology and services procurements

Figure 2. FGDC's GIRM Supports the U.S. Federal Enterprise Architecture.

While the process for inclusion may vary in other nations, the CICE and ORM Architectures will serve as a mechanism for incorporating geospatial functionality and geoprocessing specifications into National-level Information Technology and Electronic Government Architectures. Opportunities for such actions exist in nations such as Canada, the Netherlands, the United States of America, and other nations, which either currently have or are developing National Architectures.

2.2 Relation To Spatial Data Infrastructures

Around the world over 50 Nations are developing Spatial Data Infrastructures to help them improve their ability to find, access and more effectively use geospatial information and technology in their governmental and business activities. These national activities are supported by regional collaborative efforts in Asia and the Pacific, Europe, the Americas and Africa and an emerging Global Spatial Data Infrastructure (GSDI) effort.

While there are many differences in economic, social and legal frameworks around the world, the GSDI is being fueled by widespread agreement on common approaches in many fundamental Spatial Data Infrastructure development and implementation practices. Through the coordination efforts of the Global Spatial Data Infrastructure Steering Committee (now the GSDI

Association), the GSDI is taking on a clear form and substance. It consists of standardized Geospatial Metadata, a Network of Spatial Data Clearinghouses operating on common standards based protocols, an emerging agreement on a set of core data sets that will be globally available to serve as base data for SDI linkage, for common use in spatial data applications, and for further attribution and densification for larger scale use. Figure 3 depicts critical aspects of the GSDI. It is enabled by common standards and architectures which are developed / endorsed by international, national and voluntary standards organizations. The GSDI is made up of an array of local, national and regional spatial data infrastructures supporting user's needs for spatial data and services. SDI's further support a wide variety of user applications and maintain consistent growth in their utility through user interaction and constant infusion of new or refreshed data resources and an improving set of services and applications.

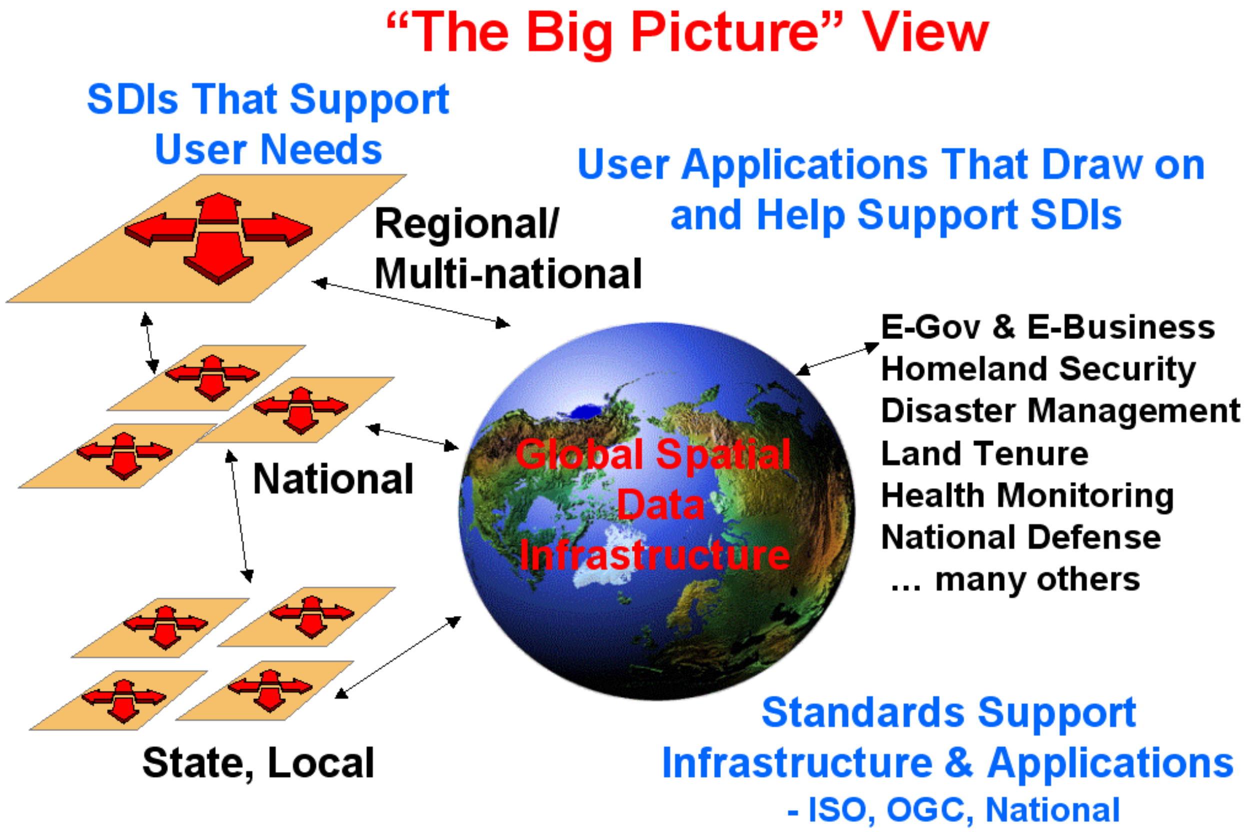


Figure 3. Standards-based COTS directly support SDI.

Geoff – same as in the other figure I don't seem to be able to change this. I wanted to change "Global" on the Globe to "Global Spatial Data Infrastructure"

A final and equally critical component is the emergence of a common geoprocessing technology architecture for use around the world in spatially enabling government and business enterprises. The CICE feeds this technical architecture and provides real examples of application of interoperable Geospatial technology specifications and, through the OGC Specifications Program, the specifications themselves that are incorporated into the Information Technology Architectures identified above.

3 CICE Enterprise Viewpoint

The Critical Infrastructure Collaborative Environment (CICE) Architecture is based on the need to enhance the ability of organizations and individuals to use geospatial processing technologies in an open distributed processing environment to address issues associated with assuring the continuity, viability and protection of critical infrastructure.

This open distributed architecture for CICE will be described from four non-overlapping viewpoints. These viewpoints are: Enterprise; Information; Computational; and Engineering viewpoints. This collection of interrelated viewpoints will provide for the development of the CICE as an initiative that supports multiple technology goals within a business / mission-based structure. It will also provide a way of ensuring that that the elements of the CICE become incorporated into the OGC Reference Model, Federal / National Reference Models and other appropriate models, so that specifications based reusable elements can be adopted for common use, not only within the Critical Infrastructure Community, but also within the entire geospatial information community. CICE will be a source of new business needs, specifications requirements, initiative and specifications for the ORM. These additions to the ORM will be incorporated through established OGC procedures for updating and maintaining the ORM.

This description focuses on the Enterprise or Business perspective. The Enterprise viewpoint is concerned with the purpose and scope of critical infrastructure protection and how it relates to the overall business areas of responsibility of government and the service specifications of government. It will also cover the primary roles and interactions required to use interoperable geospatial information and technology in a dynamic, distributed, information-sharing environment. The Enterprise Viewpoint has focused on government lines of business and business needs, but also is intended to address private sector needs. While there is no comparable private sector Business Reference Model to the government models used, it is anticipated that the Enterprise Viewpoint will cover many of the key business functions involving geospatial processes that are transacted in the private sector.

3.1 Critical Infrastructure Communities of Practice

The Critical Infrastructure Community is simultaneously a defined community of relevant and affected interests and a dynamically changing community that potentially includes all governments, business and citizens, locally or even nationally. The reason for this dynamic environment is that Critical Infrastructure Protection encompasses activities ranging from preparedness to response and recovery. Critical Infrastructure Protection includes data, applications and services that are fully accessible and open to the public; data, applications and services that require security protection for authorized users only; and data, applications and services that are a mix of open and protected inputs and outputs.

Critical Infrastructure Protection also requires a combination of pre-identified and assured data, applications and services along with access to the full range of data and services that are and will increasingly become available through a robust set of compatible and interoperable spatial data infrastructures.

The scope of Critical Infrastructure Protection ranges from local to national and global levels and can include all sectors. However, for the purposes of describing an Enterprise view of the CICE, the scope of relevant and affected communities will be focused on the geospatial requirements necessary for assuring the protection of critical facilities, networks, systems and assets that are defined in national critical infrastructure policies.

Crucial to the success of the CICE Architecture is a design that facilitates and accelerates the development of spatial data infrastructures that are compatible and enhance the use of geospatial processing technologies as enabling technologies for these spatial infrastructures from local levels of government to national and global levels of implementation and use. The United States and Canada have active efforts within their national governments to focus policy attention and programmatic effort to assuring protection of critical facilities, networks, systems and assets. Each has defined, at the national level, the major components of its critical infrastructure. For the purposes of the Enterprise Viewpoint, Critical Infrastructure Communities will be described as follows.

3.1.1 Community Types

Two types of domain Critical Infrastructure communities exist: Domain Communities and Federation Communities. These communities may be created, modified, or disbanded at any moment in their lifecycle.

3.1.1.1 Domain Communities

A Critical Infrastructure domain community is one made up of organizations and individuals that have a common interest around a set of functional activities, a local geography, or responsibilities for similar operations. In the CICE Enterprise, there can be an almost unlimited number of Domain Communities, which could form to address interests or concerns. These Communities will be formed based on need and will be disbanded when that need is addressed or their purpose is no longer needed.

Domain Communities form a basic foundation for organizing an Enterprise architecture. Therefore a relatively stable set of communities is needed to describe the enterprise. Within the Critical Infrastructure Protection set of potential communities, there is a growing agreement on the definition of Critical Infrastructure Sectors. In several countries, Critical Infrastructure Sectors have been defined by national level policy direction. For this description, the North American Critical Infrastructure Sectors will be used to begin this definition of Domain Communities. As the Architecture is used in other nations and global regions, Critical Infrastructure Sectors will likely be modified, but the basic elements of the Architecture is expected to remain relatively stable.

<u>North American Critical Infrastructure Communities</u>

U.S. Critical Infrastructure Sectors

The Sectors that make up the critical infrastructure as initially described by Presidential Decision Document 63 and as modified by subsequent guidance for Homeland Security program implementation are:

- Telecommunications
- Banking and Finance
- Water
- Transportation
- Emergency Services
- Public Health
- Energy
- Defense Industrial Base
- Agriculture and Food
- Chemical Industry and Hazardous Materials
- Postal and Shipping
- Key Assets

Canadian Critical Infrastructure Sectors

Canadian Critical Infrastructure Sectors described by the Office of Critical Infrastructure Protection and Emergency Preparedness are:

- Energy and Utilities (such as electrical power, natural gas and oil transmission systems
- Communications (such as telecommunications, and broadcasting systems)
- Services (such as financial services, food distribution, and health care)
- Transportation (including air, rail, marine and surface)
- Safety (such as nuclear safety, search and rescue, emergency services)
- Government (including major government facilities, information networks or assets)

Commonality of U.S. and Canadian Infrastructure Sectors

While the two countries have identified their critical infrastructure sectors in somewhat different terms, there is common coverage for civil sectors. The primary difference is that the U.S. has identified Foreign Intelligence, Foreign Affairs and National Defense as Critical Infrastructure Sectors while Canada has not.

From these relationships, a new consolidated set of eleven Critical Infrastructure Sectors was identified. This set includes all of the Sectors from the U.S. and Canada and is used only for the purposes of further analysis of the relationship of Critical Infrastructure Protection to government lines of business and government business drivers. This consolidated set of Critical Infrastructure Sectors is:

- Communications
- Energy and utilities
- Financial Services
- Transportation
- Law Enforcement
- Fire
- Government Operations
- Public health and Services
- Internal Security
- Foreign Intelligence and Affairs
- National Defense

3.1.1.2 Federation Communities

A CICE Federation Community is a larger grouping of Domain Communities. It contains two or more members from Domain Communities. For CICE, there are a number of ways in which Federation Communities could be envisioned. They could consist of groupings of Sector Domains from a number of nations. They could also consist of groupings of different sectors into multi-sector Federations or they could be multinational Federations or regional groupings of countries. In the geospatial data community, regional groupings of nations are forming to address spatial Data infrastructure coordination and collaboration. Based on these established regional structures, CICE communities may be subdivided into five broad categories. These include:

- North American Critical Infrastructure Sectors
- European Union Critical Infrastructure Sectors
- Asia-Pacific Critical Infrastructure Sectors
- South American Critical Infrastructure Sectors
- African Critical Infrastructure Sectors

3.1.2 Community Lifecycle

3.1.2.1 Establishing a Community

Within CICE, communities are formed based upon the need of the community. Primarily, they are established based on mission responsibilities or lines of business that relate to any of the primary areas of Critical Infrastructure Protection: Preparedness, Detection, Prevention, Protection, Response and Recovery. Likewise, a Critical Infrastructure Protection Community may form based upon geographic need. While these are oriented towards geographic areas of responsibility, they will most likely be sub-structured to address lines of business and/or Critical Infrastructure Protection areas of responsibility.

3.1.2.2 Assignment Rules

Within the CICE Enterprise, behaviors for Communities are defined by each of the wide variety of Sectors or geographic areas for which a Community may exist. For most communities, the behaviors will be guided by already established protocols and business rules for interaction. For newly formed Communities which have not had previous collaborative efforts, new rules will be established based on the norms of the geographic area, or based on the consensus of the group.

3.1.2.3 Changes in a Community

Due to the nature of Critical infrastructure Protection, the CICE Environment will be flexible and subject to change. A Community will change depending on the needs of the members and organizations and individuals will be added or deleted, rules can be modified to meet new circumstances and an established Community may evolve to a new Community as its membership and situation changes. Such changes will be generally be achieved in a consensus process and will be focused towards meeting the broadest range of needs as possible of those interested parties.

3.1.2.4 Disbanding a Community

An established Community can disband as it completes its agreed upon tasks, meets its objectives, or otherwise no longer is needed. The members will make, for the most part, such determinations, but situations may exist where some other authority may disband a Community particularly where it was established by a specified authority.

3.1.3 Communities of Interoperability

Organizations implement a wide range of security policies and technologies, making it difficult to impose a common solution to allow direct interoperability between any two nodes. For this reason, the concept of "interoperable communities" has been proposed to allow direct interconnections between communities as well as through the hubs (Figure 4). This allows for multiple routes to be established between any two nodes.

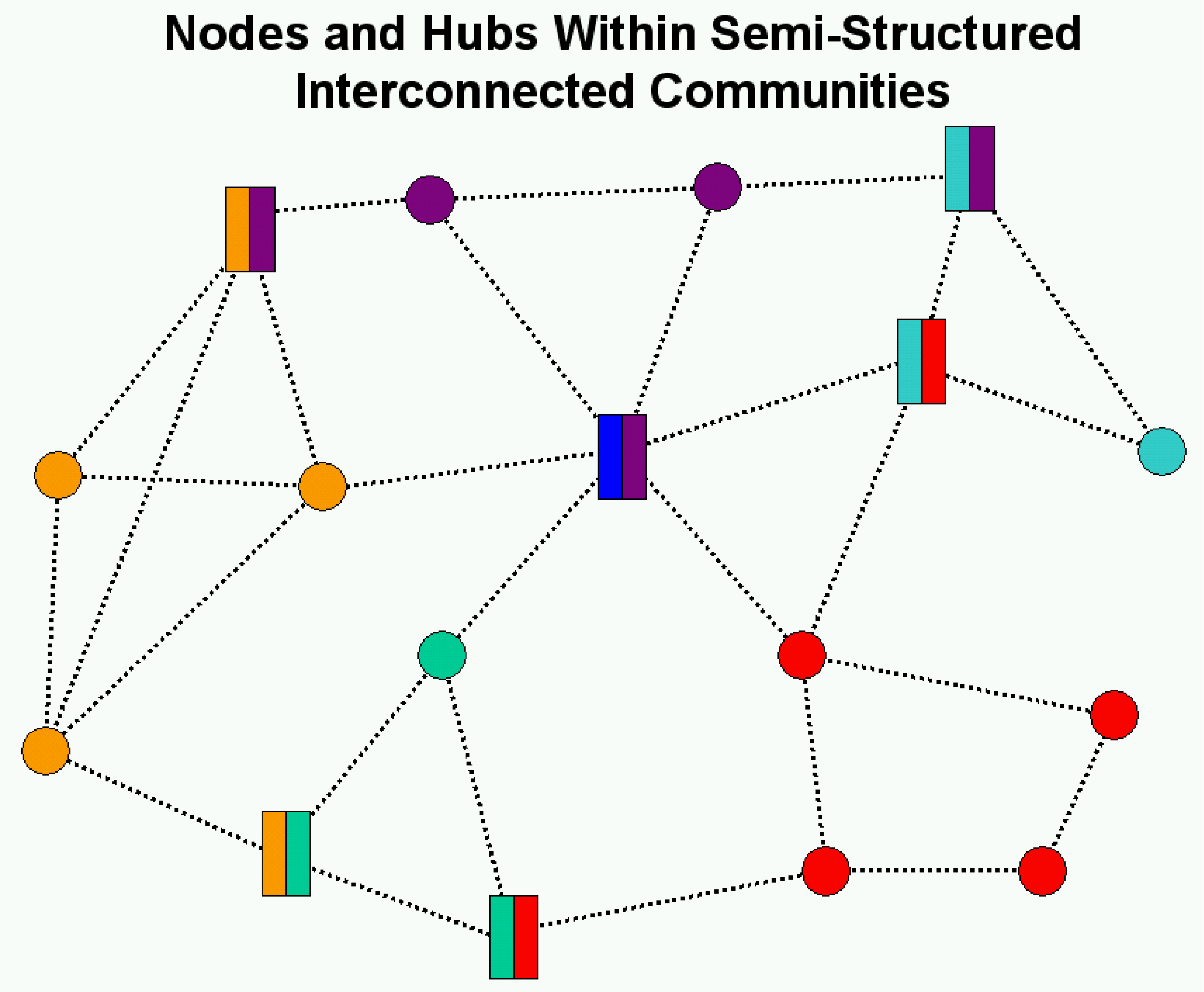

Nodes and Hubs Within Semi-Structured Interconnected Communities

Figure 4. Node and Hub Concept.

At a low-level, a "node" is a physical system on a network, including the computer and operating system. In reality, a node is the physical system within any given enterprise that is able to interact with other enterprise systems, both internal and external.

A "hub" is a type of node that is able to serve as a bridge between discrete communities. This bridge allows each community to "interoperate" between one another. A hub is able to negotiate between two or more interoperability agreements, which represent data exchange policies within an enterprise or community. The interconnections within a semi-structured interoperable community allows direct connection between communities as well as through hubs. This approach provides multiple routes between any two nodes and can accommodate a higher degree of fault tolerance than a structured and rigid interoperable community concept.

All nodes within the CICE community will join “Interoperable Communities”. Each Interoperable Community will enact and enforce it’s own set of interoperability agreements. Each node and Interoperable Community can belong to one or more Interoperable Community. A “core” set of interoperability agreements provide the nucleus around which Interoperable Communities can grow. The bridge between communities is known as a “portal”.

3.1.4 Community Characteristics

3.1.4.1 Objectives

The objective of Critical infrastructure protection is to ensure that citizens and critical resources and assets are protected to the greatest degree feasible from damage from natural or anthropogenic forces. Within a structured government environment the processes for this protection is a component of the business activities of that government. As Government Architectures are developed, Critical Infrastructure Protection specifications can be closely tied to the Government-wide Architectures.

3.1.4.2 Behaviors

Behaviors for the use of geospatial information and technologies in meeting the Business Needs of Critical Infrastructure Protection are grounded in the needs of government to provide information and services to responders and others who need geospatial resources and functionality to detect, prevent, protect, respond and recover from potential threats to critical infrastructure assets. In order for the CICE to address a wide range of government business activities, it must accommodate all of governments’ business drivers in a shifting array of access needs of the public and government authorized users.

3.1.4.3 Policies

A wide range of organizations will establish policies within the CICE. These will be established within the framework of national law, administrative regulation or by regional or local law or ordinance. Within CICE, policy statements will usually be in the form of community agreements for service specifications, data specifications, and access/security requirements for the specific needs of the community. Policy changes may affect the structure of the CICE Enterprise however, the makeup of the Architecture is such that it will be able to accommodate policy changes while still maintaining its basic operating environment and structure.

4 Operational Concept

The CICE Enterprise view supports the Business Reference Model of the U.S. Federal Enterprise Architecture and Government of Canada Federated Architecture. Both of these National Government Information Architectures are meeting the needs of the key business drivers or lines of business within government. Each has identified the business requirements differently, however, taken in totality the Common Requirements Vision (which includes Business Drivers and Business Information Requirements) of Canada and the Business Reference Model of the United States specify a full set of business areas and service requirements that can be applied to the CICE.

The U.S. Business Reference Model identifies three business areas; Service to Citizens, Support Delivery of Services, and Internal Operations and Infrastructure. For the CICE, the Services to Citizens Business Area is a primary focus as it includes the mission or program goods and/or benefits that are part of the U.S. Federal Government responsibility. However, in assessing all of the potential components of critical infrastructure protection, all three Business Areas must be considered.

In order to better understand the link of Critical Infrastructure Protection to government business, each Critical Infrastructure Sector was reviewed in relation to the lines of business identified by the U.S. BRM. The survey indicated approximately 75% of the lines of business are related to Critical Infrastructure Sectors.

Critical Infrastructure Protection is firmly embedded in government Lines of Business, and is a fundamental part of the business requirements of both Canada and the United States by being a part of 75% of government's lines of business and by requiring the information technology functionality of all of the identified business drivers.

Three roles have been identified to illustrate how Critical Infrastructure Business requirements can be fulfilled based upon the standard Web Services Architecture. These include:

> Provider – An entity that has data/information or services that will be made available for critical infrastructure activities.
>
> Requester – An entity that has a need for critical infrastructure data/information or services.
>
> Broker - An entity that provides information technology or information management capabilities for critical infrastructure activities that connects requesters and providers or which provide capabilities for the operation of the infrastructure.

The CICE Architecture is based on a publish, find, and bind pattern. This concept supports the dynamic binding between service providers and requestors since sites and applications are frequently changing in a distributed environment. These essential kinds of Web Services operations include:

> Publish: used to advertise data and services to a broker (such as registry, catalog or clearinghouse). A service provider contacts the service broker to publish (or un-publish) a service. A service provider typically publishes to the broker metadata describing its capabilities and network address.
>
> Find: used by service requestors to locate specific service types or instances. Service requestors describe the kinds of services they're looking for to the broker and the broker responds by delivering the results that match the request. Service requestors typically use metadata published to the broker to find service providers of interest.
>
> Bind: used when a service requestor and a service provider negotiate, as appropriate, so the requestor can access and invoke services of the provider. A service requestor typically uses service metadata provided by the broker to bind to a service provider. The service requestor can either use a proxy generator to generate the code that can bind to the service, or can use the service description to manually implement the binding before accessing that service.

Any given organization may assume one or more of these roles depending upon their business requirements. For example, an agency may publish data to a node, making it available for consumption by authorized agents. An authorized user in another organization would then issue a request to discover or find data relevant to the mission requirements. The user application may bind directly to the data provider if known, or a broker may assist in discovery of relevant datasets (Figure 5).

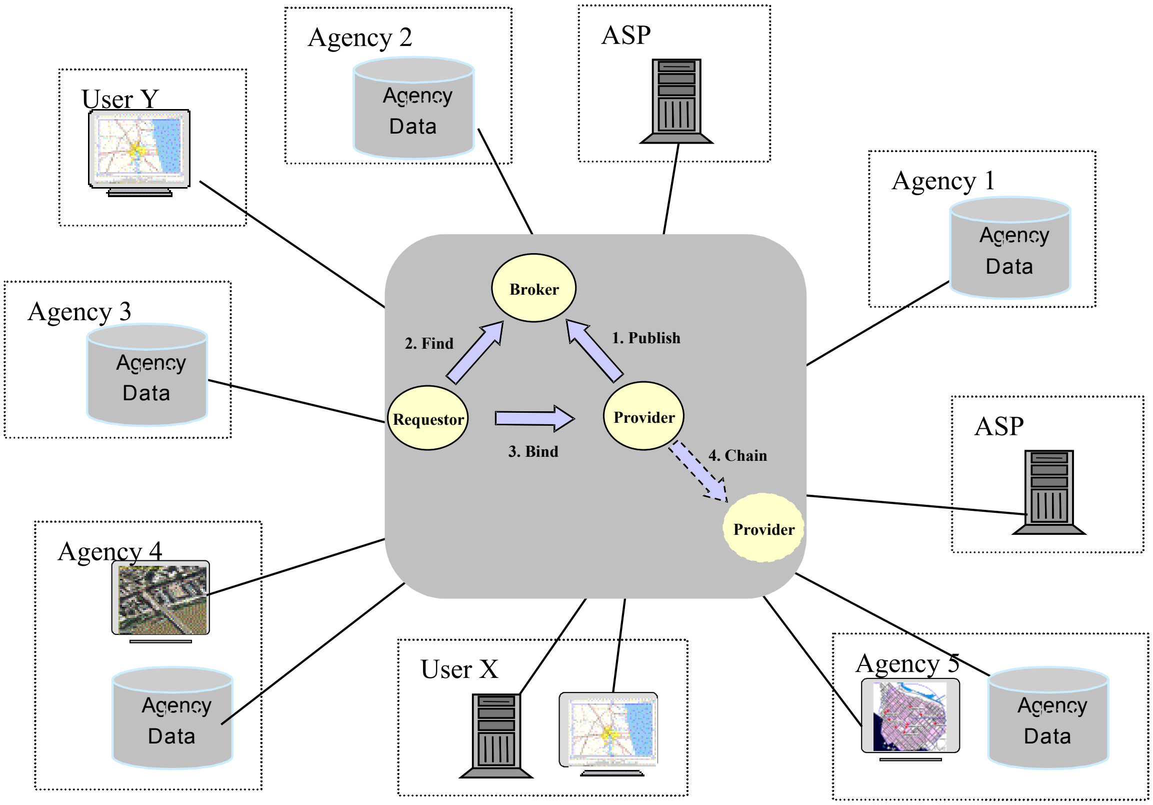


Figure 5. CIPI Enterprise Architecture Operational Context.

5 CICE Quality of Service

Quality of service is an important factor in meeting the expectations of the stakeholders of a system. The users of a system are typically not concerned with performance degradations in one aspect of a system, so long as the system as a whole performs to their overall expectations.

5.1.1 Requirements on the Enterprise

Several key elements will allow the CICE system to meet stakeholder expectations. These include availability, reliability, and security. Availability is the system's ability to be ready for use, it's performance capabilities, and it's accessibility. A system's reliability includes it's ability to be fault tolerant, meaning that there are no single points of failure, allowing the user to continue their use of the system. Security is the ability for the system to preserve the integrity and confidentiality of the information.

5.1.2 Requirements on Enterprise Interactions

The successful interaction between enterprises and exchange of information relies on several characteristics. These Quality of Service characteristics include:

Freshness - how up-to-date the information is (relevant to time-dependent information);

Precision - with what granularity the information is expressed;

Timeliness - requirements for request/response delays;

Capacity – throughput;

Accuracy - error probability;

Security - access control, integrity, confidentiality, authentication, non-repudiation; and

Precedence - the sense of the importance of the interaction relative to others (for use in cases of shortage of resources or conflicts).

In the case of the CICE, information is required to be up-to-date, precise, timely, accurate, and secure. The CICE Architecture needs to support these characteristics in order to provide relevant information to system stakeholders (Table 1).

Table 1. Quality of Service Characteristics, Business Requirements, Roles, and Functions.

Functionality	CICE Business Requirement	Player	Role	CICE Functions
1. Accessibility	A. Provide catalogue of critical infrastructure information and services	Provider	Document data, install interfaces, and post data/services on NSDI compatible network	All
	B. Identify information and services needed	Requestor Planner First Responder	Determine nature of event and type of info/service needed	Planner - All First Responder - Immediate for First Responder
	C. Make request for service or information	Requestor	Submit request for info/services based on need	All
2. Security	A. Provide information about requestor	Requestor & Broker	Requestor provides basic identification to support request	All
	B.Match requestor information to public access security schema for critical infrastructure information and services	Broker	Conducts analysis of submitted information and security requirements for info/services requested	All Immediate for First Responder
	C. Approve or deny access to information and services	Broker	Based on pre-established criteria either approve or deny	All Immediate for First Responder
	D. Audit transactions to ensure ability to recreate business events and assure correct levels of access	Broker	Maintain procedures for capturing transaction information	All
3. Client Centered Service Delivery	A. Provide current data/information, services and presentation based on requesters requirements	Provider Planner Responders Broker	Provider supplies information to meet needs identified in the request. Broker provides services and presentation to the requestor.	All Immediate for First Responder
	B. Provide feedback to requester about availability of information and services to meet request	Broker	Information to let requester know how long it will take to fulfill the request	All Immediate for First Responder
	C. Provide status information on request	Broker	Keep the requester informed about the request	All Immediate for First Responder
	D. Assure protection of personal privacy information as well as protected critical infrastructure information	Infrastructure Broker	Infrastructure coordinators establish protocols. Brokers implement protocols to ensure appropriate levels of privacy.	All

Functionality	CICE Business Requirement	Player	Role	CICE Functions
4. Effective and Efficient Service Delivery	A. Provide information about actual performance of service delivery	Infrastructure Broker	Infrastructure coordinators establish mechanisms, Brokers implement	All
	B. Maintain and improve data/information and services availability, the infrastructure and architecture	Provider Requester Broker Infrastructure	Provider improve quality, reliability, standardization and access to data and services. Requestor improve understanding of needs, common requirements and pre-plan as much as possible. Brokers improve interfaces and tools. Infrastructure coordinators continue to provide guidance and capabilities to evolve the infrastructure and implement new architectures.	All

6 CICE Use Case Narratives

6.1 System Concept: Cross Border Project

For the CIPI-1 Initiative, a demonstration capability was developed around a realistic but fictional scenario involving chemical release along a major international transportation corridor. This scenario would require response and recovery activities from local, state, provincial, and national agencies, as well as coordination between nations at an international level. The following narrative describes the situation:

At 9:30 AM the Windsor, Ontario Police Department receives a report from the Mitchell Park area that a very heavy scent of chlorine gas has been detected in the air by local citizens. While sending a patrol unit to respond a second call is received reporting the same heavy scent of chlorine gas 2 kilometers to the Southwest of Mitchell Park, and then a third near the intersection of Tecumseh and Huron. The reports are plotted on a map, along with reported potential sightings of a commercial truck in the area.

Concern develops that this commercial truck, enroute to the U.S. via either the Ambassador Bridge or the Detroit-Windsor Tunnel, may be leaking its chlorine gas contents unknown to the driver. The UN Codes for chlorine gas and other gaseous chlorine compounds are determined and cross matched to the City of Windsor's database of known hazardous materials. The resulting list of three chemicals and their respective UN Codes are then broadcast to local law enforcement, and emergency response forces in the Windsor and Detroit area.

A series of notifications about this event are immediately communicated involving the Windsor Police, Canadian Customs, local Hazmat Response Teams (HMRT), the Ontario Provincial Police, the RCMP, the Ontario Emergency Measures Organization, the Federal Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), and DND. Uncertain of the intent of the driver of the truck and his planned destination, the Detroit police are notified, which in turn triggers notifications on the United States side to the Detroit local Hazmat and terrorist response units, U.S. Customs, the Michigan Emergency Office, FEMA and NIMA.

The Windsor EOC and the Wayne County EOC become the lead national Emergency Operations Centers (EOC) for Canada and the U.S. respectively. These lead EOCs serve to coordinate all activities and through co-production provide a continuously up-dated situation picture to all authorized responders. A specialized situation picture is provided to the media. Critical response teams are dispatched to the vehicle scene and to secure the Windsor-Detroit border crossings.

The Windsor Police determine that the truck is tracking toward the Ambassador Bridge. Nearing the border crossing plaza the truck is stopped by authorities to prevent further travel, and isolate the vehicle to minimize the damage. The truck, now disabled, rests 300 yards from the river on the Canadian side of the border. Authorities assess and project the threat areas that could be affected by the developing situation and issue a second series of public alerts to targeted groups and locations to maintain awareness of the developing situation and to direct actions such as evacuation and sheltering in place.

The interfaces leveraged by first responders, EOC staff, and other local, state, and national officials should allow the user to access public, framework data (location, name, imagery etc) and have a protected area for more sensitive data (load classification, traffic flow and density and any vulnerability information). The users, based on their access permissions, would be able to see either the framework data only or a combination of the open source and protected information. Within the protected area, there would be varying degrees of permissions based on the role of the organization. The vast majority of the information is available from a variety of government and private sector sources.

The information requirements to deal with this situation will vary, both from between countries and between the various levels of government. However, decision makers at all levels of government would be asking for data concerning the situation and information on the border crossings as well as population, traffic and weather information.

Security managers and law enforcement agencies will need to track the vehicle and access protected information dealing with the vulnerabilities of the border crossings in the areas and the deployment of police and customs resources. They will also need to have detailed information on the overall geographic layout of the border crossing area. Once the truck reaches the border crossing, they will need to establish a security perimeter and be able to share that information with a variety of groups.

Critical Infrastructure protection officials at all levels of government would require a modeling capability to present the most likely routes the driver could take, or potential impact to the area's population. They would also have to overlay this information on accurate framework data covering not only the roads, but also the population and basic infrastructure information. As well, they would also have to have access to protected information on vulnerabilities and infrastructure information. They would also have to have access to DEMs and Imagery for the border area in both medium (10-25m resolution) and high (1 to 4m resolution) in order to assist their analysis and their presentation of the information to decision makers.

If the vehicle is severely, or it appears likely that it sustained significant damage and the chemical is released, the consequence managers at the various levels of government will require information in order to deal with the situation. Local officials have to be able to determine which areas may be affected, so they will need access to detailed street and population information on both sides of the border. Provincial, state and federal officials will have to be able to access the local information in order to make decisions concerning the deployment of additional resources.

Finally, throughout this scenario, there is a requirement for information to be fed to the media. This application should have the capability to seamlessly send approved, unclassified information to a web site that could be accessed by the media.

In this Cross Border scenario, a wide range of disaster management (DM) and emergency response (ER) activities are undertaken. Many activities require geospatial support for data accessibility, data fusion, and security. Recognition of all activities is important from the perspective that they may place constraints (e.g., timing and sequence) on geospatial-oriented activities.

6.1.1 Actors

There are three main classes of actors described in these activities:

- The Media
- The Lead Emergency Operations Centers (EOC) of which there is one for Canada and one for the U.S. During this type of cross border incident, EOCs will likely be activated in all municipalities in the area of concern and at the state and provincial levels. One EOC in each country will be designated as the lead to coordinate all activities. It is assumed that these EOCs will provide the main portals for geospatial information for the scenario.
- Federal Emergency Centers. It is assumed that for Canada, this agency will be the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) with support from the Department of National Defense (DND) J2 Geomatics & Imagery. In the U.S. it is assumed this agency will be the Federal Emergency Management Agency (FEMA) with support from the United States Geological Survey (USGS) and U.S. Department of Defense (DOD) agencies. The prime role of the Federal Emergency Centers is to access data, enforce information security policies, and to provide support in consequence assessment.

There will be additional classes of actors in these activities including:

- First Responders
- Authorized Responders
- Municipal Police
- Police Dispatchers
- Hazardous Materials Response Team
- Threat Assessment Teams
- National Counter-Terrorist Organizations
- Public Alerting System Coordinator

- Residents/Occupants

6.1.2 Services

The classes of service described in these activities are:

- Data Access Services. These are the services that provide access to the data needed by the actors.

- Presentation Services receive data from Data Access Services, fuse that data and render it for display to the user.

- Discovery Services provide a means for users to locate needed data and services.

- Client Services provide a user interface and user-side logic for interfacing with the other classes of service. The concept of a "situation picture" or "common operational picture" is introduced here as the main geospatial information product from multi-source fusion of intelligence

6.1.3 Information

The classes of information described in these activities are:

- Vector data

- Imagery data

- Gridded data

- Video data

6.2 System Concept: Banking and Finance Sector

This Use Case Narrative is focused on the Banking and Finance Sector and depicts a possible scenario that involves the high-level functionality and business requirements described for the CICE Enterprise Architecture. However, while the initial emphasis is on the Banking and Financial Sector, the Use Case will demonstrate the need to quickly involve other Sectors of the CICE Community.

A concerted effort is launched to disrupt the Banking and Financial markets of the world. These efforts are both electronic and physical disruption primarily in G8 nations. Major efforts from unknown sources are initiated to disrupt the electronic flow of information at major financial markets in G8 Nations. These cyber attacks are quickly followed by bank robberies in the U.S., Canada, and Germany. Over 10 robberies, often accompanied by violence and loss of life, are carried out within hours of the cyber attacks. The intent of the attacks is to shut down the flow of financial resources and business transactions and to create fear about the safety of citizens conducting normal daily personal banking chores.

As the attacks begin, there is an immediate need for Accessibility to Critical Infrastructure geospatial information. The Banking and Financial sector have the need to know where the cyber attacks are occurring geographically and to map electronic network information spatially to detect patterns and to identify potential sources of the attacks. As the bank robberies begin to occur, they will likely be perceived as individual incidents, but as information is entered real time into law enforcement databases, a larger picture will quickly emerge. In order to respond locally and understand the picture nationally and globally, access to geospatial information is necessary.

Security functions are critical as protected financial information will be required to assess and respond to the situation. Sensitive or classified information about terrorist organizations will also rapidly come into play and will need to be disseminated and used with great caution, but among a large number of dispersed users nationally and globally.

A large set of Client Centered Service Delivery mechanisms will need to be deployed. The requestors' requirements for these services will be different depending on the portions of the attack that they are dealing with. However, on a cumulative basis virtually all services of Spatial Data Infrastructures will be needed and with immediate and correct response in terms of Effective and Efficient Service Delivery.

In responding to the global cyber attacks and to the local bank robberies, the following sectors, at a minimum, will be intimately involved:

Banking and Financial – Sector initially attacked

Communications - Telecommunications networks under attack

Energy and Utilities – Provide the physical infrastructure for telecommunications and other electronics networks

Law enforcement – Responding to Bank robberies

Transportation – Potential escape routes for perpetrators of the Robberies

Government Operations – To protect the integrity of national financial systems and market operations

Key assets – Key facilities and commercial locations

National Defense – Due to the global nature of the events immediate National Defense, Security, Foreign Intelligence and Diplomatic involvement is required.

6.2.1 Actors

Use case actors can be identified in the following Domain Communities:

- Banking and Financial community
- Law Enforcement community
- Government Operations community
- National Defense community

6.2.2 Services

The classes of service described in these activities are:

- Data Access Services. These are the services that provide access to the data needed by the actors.
- Presentation Services receive data from Data Access Services, fuse that data and render it for display to the user.
- Discovery Services provide a means for users to locate needed data and services.

6.2.3 Information

The classes of information described in these activities are:

- Vector data
- Imagery data
- Gridded data
- Video data

Bibliography

[1] IETF/RFC 2119. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997. Available [online]: <http://www.ietf.org/rfc/rfc2119.txt>.

[2] IETF/RFC 2828. *Internet Security Glossary*. May 2000. Available [online]: <http://www.ietf.org/rfc/rfc2828.txt>.

[3] ISO/IEC 9594-8:2001. *Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.* [also published as ITU-T Recommendation X.509 (03/00)].