• Introductions
• IEF Overview (10-15 minutes)
  – Key Concepts
  – Alignment with I2F
  – Alignment to five (5) Whitehouse Information Sharing and Safeguarding Goals
• Policy Based Access & Release Control (30-40 Minutes)
  – Presentation & Demonstration
• Policy Based Structured Messaging (30-45 Minutes)
  – Presentation & Demonstration
• Questions & Answers (as desired by audience)
IEF Objectives
(To Address Multifaceted Domain)

• Reference Architecture and standards for and Integration layer that provides Policy-Driven Data-Centric information sharing and safeguarding (ISS)solutions that target:
  – Information & Decision Advantage
    • Responsible Information Sharing
    • Coordinated Information Sharing
    • Quality Information
  – Dynamic Interoperability
  – Defense in Depth
  – Rapid Policy Development and Deployment
  – Shared, Repurposeable Services and Infrastructure
  – Open International Standards
    • Multiple product vendors
    • Multiple Sources for SMEs
    • Support ecosystem

• Service and Interface Specifications that integrate user specified products and services to deliver responsible Information sharing solutions
Focus of the IEF RA

• Integration Layer for User defined Information Assurance Services that Deliver Defence-in-depth for ISS Services

• Information exchange Policy Vocabularies
  – Family of Vocabularies
  – Supporting Modeling Profiles

• High level Requirements for Policy-driven Data –centric Services
  – Identity, Credential and access Management (ICAM)
  – Access / Release decision and control Information Packaging and Processing
  – Trusted Auditing

• Service Interfaces (as needed)
  – Information Dissemination Services
  – Platform/Network Security Services
  – Platform / Network Services
  – Communications
IEF Reference Architecture

Operational Capabilities

Shared Files Store
- Controlled Access to individual services, directories and files based on user policy rights and files sensitivities
- Alerts and Warnings on Unauthorised Actions

E-Mail
- On send, verify access rights:
  - For each Recipient to receive the content of email and each attachment
  - For the Sender to send the content email and each of the attachments
- On receipt, verify access rights to the content of the email and each of the attachments

Instant Messaging
- Encrypted Chat Sessions
- Unique encryption for individual message to enable private message within a chat session

Web Services
- Selective inclusion of content within a message based on requesters policy rights
- Verification of the user’s policy rights to publish the specific content to the web or cloud.
- Verifies the user’s policy rights to receive

Messaging Middleware
- Selective inclusion of content within a message
- Verification of senders policy right to send the specific content to the selected communications channel
- Verification of each recipients policy rights to access the content of the message (dependent on selected middleware)

Access, Action & Release Control Services

Information Sharing Agreements
Format releasable data set to sharing agreement message protocol
Route formatted message / document to approved communication channel

Assemble of data to accommodate sender and recipient authorizations:
- Aggregate data and information elements
- Transform data elements to conform to sharing agreements
- Mark data based on structure and/or data values
- Redact/Filter data to reduce sensitivity or address QoS

Parse, Process (validate data and transform data) and marshal data

Data / Information Packaging

User Data Stores

Access Control Policies

Packaging & Processing Policy
I2F Architecture Framework

- Security Elements are required for each Architectural Domain
- Performance is typically integrated into part of System and Application Architecture
- Enabling organizational and community governance is will be a critical success factor and a measure of maturity
- Requires Performance Monitoring and Security Auditing
- IEF is providing standards that bind the Architectural Domains through alignment with UPDM

Policy Instruments:
- Legislation
- Regulation
- Policy
- Service Level Agreements
- Memorandum of Understanding
- Standard Operating Procedures

IEF is providing traceability through integration with EA Frameworks and Tools

IEF Increases alignment to National Strategy on Information Sharing and Safeguarding
IEF borrowed validation and verification criteria from the Public Safety Canada Interoperability Continuum (9 capability areas)

Which in turn borrowed from the DHS SAFECOM Interoperability Continuum (5 Capability areas)

The PSC Continuum added focus to the information Management, Architecture and ISS elements

The continuums may provide a foundation for the I2F Interoperability Maturity Model
The policy models integrate the domain vocabularies
Policy models align policy to the data domain

The goal is to translate policy models into a machine readable and executable form
Deliver increasing levels of policy automation
Enable dynamic control of policies at runtime

Policy has a life cycle
Policy Models provide alignment to other Architectural components
Architecture enables governance

Policy is enforced against the specific values of the data at run-time
Policy is applied based on the Data Sensitivity of the specific information element
Data and metadata elements are govern the application of policy

IEF Increases aligns Information ISS Policy to ISS processes, ISS services and Data holdings.
1. Drive Collective Action through Collaboration and Accountability.
   - Architecture models provide data that informs governance
   - Architecture and Tamper-resistant logs enables design audits, modeling & simulation, and forensic auditing
   - Policy driven approach enable the deployment of shared/common services the automate user specified rules

2. Improve Information Discovery and Access through Common Standards
   - Packaging service enables greater tagging of documents and messages during assembly
   - Integration of sharing & safeguarding during packaging enables the use of standards messages (e.g., schemas)
   - Architecture and Tamper-resistant logs enables certification

3. Optimize Mission Effectiveness through Shared Services and Interoperability
   - Policy driven solutions enable the deployment of shared services and Infrastructure
   - Standards based approach promotes:
     • multiple vendors and increased competition
     • Portability across vendor solutions

4. Strengthen Information Safeguarding through Structural Reform, Policy, and Technical Solutions.
   - Authorizing sender and recipient prior to information release mitigates insider threats
   - Data-centric services enforce policy (control release) at the data level
   - Tamper resistant logging support real-time monitoring and forensic auditing

5. Protect Privacy, Civil Rights, and Civil Liberties through Consistency and Compliance
   - Policy driven services provide greater fidelity in the application of privacy and security rules
   - Tamper resistant logging of all transactions promote greater accountability and conformance
Questions and Answers

- General IEF Concepts and Objectives
- Alignment to I2F / Project Interoperability
- White House Information Sharing and Safeguarding Strategy
The Information Exchange Framework (IEF)

Key Features / Take-away

- **Access & Release control for information exchanged using:**
  - File Share
  - Email
  - Instant Messaging
  - Message Bus
  - Web or other distribution Service

- **Policy Driven:** Derived from and Traceable to Policy Instruments

- **Data Centric:** Enforces policy at the data level

- **Dynamic Policy Management and Administration**
  - Ability to adapt policy environment to address dynamic real-world operational requirements
Dr. Daniel Charlebois will demonstrate the SAMSON Technology Demonstrator (TDP)

Mike will demonstration Situational Awareness using:
- World Wind (NASA) GIS
- Policy Driven Data Aggregation Service (To Be OMG Standard)
- SOPES IEDM (OMG Policy Model Specification) / IEPPV (OMG Standard)
- JC3IEDM (NATO STANAG 5525)
- Open Splice (OMG DDS Standards based Open Source)
Any Quick Questions
• Policy Driven data Centric Access & Release Control
  – File sharing
  – Email
  – Instant Messaging

• Key Concepts
  – Policy Driven
  – Data Centric
  – Defence in Depth
• On the topic of structured data

• NIEM but not Necessarily NIEM
  – EDXL
  – CAP
  – HL7
  – JSON
  – MIP PDU
  – Etc .....................

BTW: we do not differentiate between data and meta-data (e.g., Marks, Tags, and Labels) in a releasable data-set / message. Just another attribute to process.
Why Common Messaging & Why so Challenging

- Why Common Messaging
  - Common Community Message Semantics, Syntax and Format (NIEM, EDXL, HL7, ..., ADATP-3, OTH-gold, USMTF, ...)
  - Semantic Interoperability: the ability of two or more systems to exchange data/information elements and subsequently present that data/information to a user, such that it is understood without a loss intent, and operational context.

- Some of the Challenges
  - Multiple Information Sharing requirements / agreements
    - Differing levels of sensitivity of messages based on content (runtime data values)
    - Differing levels of trust in communication networks, systems, and users
  - Multiple planned and spontaneous missions / operations
  - Need for rapid deployment of capability
  - Changes in operational context (threat, risk, scope, roles & responsibilities, ...) that require real-time changes on information sharing and safeguarding patterns
Standardized Messages Initiatives
Primary Objectives

- Increase Community/Domain Interoperability
- Manage the number of interfaces to maintain
- Reduce Cost & Risk
How to Gain the Benefits of Common Structured Messages

• Separated Concerns
  – Preparing and releasable data set
  – Formatting for exchange
  – Release to distribution Mechanisms

• Develop reusable Information Sharing and Safeguarding Patterns

• Apply a layered set of Data Sharing and Safeguarding Policies
  – Sharing Policies
    • Data and Information Element Aggregation
    • Data Transformation
  – Safeguarding Policies
    • Selective inclusion of data elements
    • Data & Information Marking
    • Data / Information Redaction
Where is the challenge?

Data in Use

- Addressed by: Extract, Transform, Load; or Application Code

Data in Transit

- Rigid and Brittle
- Costly to Maintain and Adapt
- Not Responsive to Changes in Operations

Data at Rest

- Typically Pier-to-Pier
- Task/Organization Specific
- Stove-piped

Organizations have lost, the institutional knowledge and memory needed to manage and maintain Business Rules related to information usage and exchange.
Information Exchange Packaging Policy Vocabulary (IEPPV) Target

Application Semantics
Application Interface Specification

Community Exchange and Service Level Agreements
Community Interface Specifications
Community Exchange Semantics
Community Messaging Protocols
Community Networking and Community Specifications

Data and Information (Semantic) Patterns
- Aggregation, Parsing/Marshalling
- Static and Dynamic Filters (Security, Privacy, QoS, ...)
- Structure and data Transformations
- Data and Information Tags (Metadata)

Storage Semantic
Storage Business Rules
Store attributes and domains
Meta tags and labels
Data and information Relationships
GUIDs / DB Keys
Assembling messages that balance the information sharing and safeguarding requirements is a recursive process that is affected by changes in policy rights, data values and operational context.
Same Data Multiple Exchange Formats

ISE Layer:
Aligns the information to its format/protocol and the agreed/authorized distribution Channel.

Semantic Layer:
Groups the datasets into meaningful and releasable datasets.

Transactional Layer:
Defines rules for aggregating, transforming, marking, and redacting data and information elements in conformance to policy instruments.

Foundation Layer:
Links policy model to Physical Data Element.

Protocol Data Unit
NIEM XML
JSON Exchanges

Community Focus
Local Focus
Using Filters/Redaction to Address Releasability

- Low Trust
- Moderate Trust
- High Trust

ISE Layer:
Semantic Layer:
Transactional Layer:
Foundation Layer:

F Filter / Redaction
Using Filters/Redaction to Address Releasability

Low Trust

Moderate Trust

High Trust

ISE Layer:

Semantic Layer:

Transactional Layer:

Foundation Layer:

Filter / Redaction
Using Filters/Redaction to Address Releasability

Low Trust

Moderate Trust

High Trust

ISE Layer:

Semantic Layer:

Transactional Layer:

Foundation Layer:

Filter / Redaction
Demo Configuration

World Wind GIS

COIL TEST HARNESS

Common Object Interoperability Layer (COIL)
Technology Demonstrator

SOPES IEDM

CORBA

Memory Based Object Model

Shared Operational Picture Exchange Services Information Exchange Data Model (SOPES IEDM)

JC3IEDM/STANAG 5525

Situational Awareness Simulation

Data Distribution Service for Real-Time (DDS)

OMG Standard

NASA Open Source GIS

OMG Standard

OMG Standard

Published

Subscribe

Publish
Questions and Answers
Demonstration Objectives

• Demonstrate the ability to selectively share information with mission partners using:
  – Information Patterns to Policy Automation

• Demonstrate a Separation of Concerns:
  – ISS Infrastructure vs. Policy Automation

• Demonstrate the approaches ability to increase flexibility, agility, and sustainable

• Demonstrate Standards Based Implementation
  – ISS Policy Model / Standards Based IEPPV
  – CORBA Based Object Management
  – Execution of Information Patterns (SOPES IEDM)
  – Standardized Messaging (MIP PDU, SOPES XSD)
  – Standardized Distribution Mechanisms (DDS)
Simple Scenario

- Fire on a Navy Ship in Canadian Domestic Waters / Collaborative Response
  - Focus is on visualization not data level details

- Demonstrate Selective Information sharing across 4 government Organizations
  - DND Headquarters

- Demonstration the ability to modify distribution patterns during Operations using a serialization of architectural patterns

- Demonstrate support for multiple data formats simultaneously
  PDU (primary Distribution), SOPES XML (could be converted to a NIEM IEPD)
First of the Policy Vocabularies

- **Information Exchange Speciation (IES) Layer**
  - Information Specification
    - Message Specification (Simple form)
      - Message Metadata Specification
      - Filtered Semantic Element or Semantic Element (1..*)
      - Attachments
    - Filtered Semantic Element or Semantic Element (1..*)
      - Filtered Transactional (1..*) – identifies which attributes are filterable at runtime
  - Distribution Specification

- **Semantic Layer**

- **Transactional Layer**
  - Transactional Element (1..*)
    - Transactional Element (1..*)
    - Wrapper Elements (1..*)

- **Foundation Layer**
  - Wrapper Element (1..*)
Communities of Interest
(Based on Information Sharing Requirements)

• 4 Operational Nodes with separate Information Sharing Agreements (ISAs)

• Asynchronous information sharing agreements

• Operational Nodes can participate in multiple agreements representing virtual networks (Operations Needs, Privacy or Security Levels); in this case represented by DDS Topics
DODAF: information Exchange Element has specializations:

- Information Specification
- Filtered Semantic
- Message
### Information Exchange Specification

**1.** 2 versions of an Information Exchange Specification

**2.** 1..* Filtered can be assigned to a single specification

**3.** 1..1 Information Specification – it forms a pattern that can be used may reused under multiple IES. IES using different communication channels, protocols, ...,
Semantic Interoperability Demonstration
April 2010

Mike Abramson, ASMG Ltd.
265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1
Fax: 613-231-2556
Phone: 613-567-7097 x222
Email: abramson@asmg-ltd.com
Back-up Slides
• Adoption of IEPPV Specification
• Alignment with UPDM:
  – IEPPV
  – NIEM Profile
• Initial mapping of I2F to IEF ...
• Developed Next steps
Next Steps

- Combine the activities of the IS WG and IEF WG (C4I, MARS, add Gov) – Austin Meeting
  - Add Ashwini Jarral as co-chair
  - Leave it as a Platform Working Group to address horizontal Integration
  - Has work on the go:
    • IEPPV (Adopted Sept 2014)
    • IEF Reference Architecture – Active RFP
- Initial Assessment: Lots of commonality – but needs better alignment
  - Step 1: align concepts and terminology
  - Identify Gaps and standards opportunities
  - develop consolidated presentation and roadmap for Long beach CA
  - Step 2: review and comment on IEF Use Cases (two week from Austin)
  - Collaborate in the development of the IEF RA Submission
  - Step 3: identify & implement pilots (IE Project Interoperability Pipeline)
• **Policy Driven**: A process through which user defined policy instruments are translated into machine readable rules (/instructions) and enforced by software services and systems. This process results in full traceability from policy instrument to implementation (policy decisions and enforcement points).

• **Data Centric**: enforce policies/rules against individual data assets; often referring to metadata or tags included within an information asset.

• **Defence-in-Depth** (for data/information assets): A layering information safeguards to protects a specific information asset based on the reported value.

• **Responsible Information Sharing**: Compliant with law, regulation and policy; consistent with community and agency strategy and direction, to include protect of information, sources and methods, and civil liberties and privacy; and accountable through governance and oversight - maximize the quantity and quality of information that is discoverable and accessible to authorized users and partners.

• **Quality Information**: provision of high-quality information tailored to the needs of the decision makers’:
  - **Accurate**: Information that exactly, precisely, and correctly presents availability, usability and deploy-ability of C4ISR capability, systems and services;
  - **Authoritative**: Information that is recognized or accepted as being true or reliable;
  - **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; and
  - **Secure**: Information is protected from inadvertent or Malicious Release to unauthorized persons, systems or organizations.
• Level 6 (Conceptual): Interoperating systems at this level are completely aware of each others information, processes, contexts, and modeling assumption

• **L5(Dynamic): Interoperating systems are able to re-orient information production and consumption based on understood changes to meaning, due to changing context.** *(dynamic application of Policy)*

• L4(Pragmatic): Interoperating systems will be aware of the context (system states and processes) and meaning of information being exchanged. *(Shared Approaches and Services)*

• L3(Semantic): Interoperating systems are exchanging a set of terms that they can semantically parse and process, and convey a common or shared meaning.

• L2(Syntactic): Have an agreed protocol to exchange the right forms of data in the right order, but the meaning of data elements is not established.

• L1(Technical): Have technical connection(s) and can exchange data between systems

• L0(No): n/a

Tolk et al. The levels of conceptual interoperability model: Applying systems engineering principles to M&S. Spring Simulation Multi-conference (SpringSim'09). San Diego, CA, USA. Published by SCS in the SpringSim'09 Proceedings.

The SAFECOM Program

Interoperability Continuum

<table>
<thead>
<tr>
<th>Governance</th>
<th>Individual Agencies Working Independently</th>
<th>Informal Coordination Between Agencies</th>
<th>Key Multi-Discipline Staff Collaboration on a Regular Basis</th>
<th>Regional Committee Working within a Statewide Communications Interoperability Plan Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Operating Procedures</td>
<td>Individual Agency SOPs</td>
<td>Joint SOPs for Planned Events</td>
<td>Joint SOPs for Emergencies</td>
<td>Regional Set of Communications SOPs</td>
</tr>
<tr>
<td>Technology</td>
<td>DATA ELEMENTS</td>
<td>Swap Files</td>
<td>Common Applications</td>
<td>Custom-interfaced Applications</td>
</tr>
<tr>
<td></td>
<td>VOICE ELEMENTS</td>
<td>Swap Radios</td>
<td>Gateway</td>
<td>Shared Channels</td>
</tr>
<tr>
<td>Training &amp; Exercises</td>
<td>General Orientation on Equipment and Applications</td>
<td>Single Agency Tabletop Exercises for Key Field and Support Staff</td>
<td>Multi-Agency Tabletop Exercises for Key Field and Support Staff</td>
<td>Multi-Agency Full Functional Exercises Involving All Staff</td>
</tr>
<tr>
<td>Usage</td>
<td>Planned Events</td>
<td>Localized Emergency Incidents</td>
<td>Regional Incident Management</td>
<td>Daily Use Throughout Region</td>
</tr>
</tbody>
</table>

The Starting Points for the Emergency Management System Interoperability Continuum

Foundation for the Information exchange Framework

Maturity Continuum Across Nine (9) Capability Areas Central to ISS

Opportunity to Report Capability across the Nine Domains

Foundational Element of the IEF / Derived from SAFECOM Interoperability Continuum
IEF Interoperability Continuum

Maturity Continuum Across Nine (11) Capability Areas Central to ISS

Opportunity to Report Capability across the Nine Domains
The Emergency Management System Interoperability (EMSI) Framework is intended to provide a single, universally accessible source of information, tools, and best practices that will enable the Emergency Management and Public Safety Communities to align capability and deliver communications interoperability and information interoperability. This will enable collaboration, situational awareness, and coordination during the Planning, Response, and Recovery Phases of an operation.

The EMSI Framework will provide metrics to assist community members assess their internal capability and their ability to interoperate in local, regional, and national operations. The metrics are intended to assist stakeholders develop IM/IT strategies and roadmaps that enhance municipal, provincial, and national capability.

Roadmap Elements
- Enhanced Interoperability
- Increased Information System Capability
- Improved Information Quality and Situational Awareness

Alignment of EMSF Elements

The EMSIF Architecture Framework aligns industry best practices in Enterprise, System of Systems, and System engineering to provide the Emergency Management and Public Safety Communities with the ability to collaborate in the development of information sharing and collaboration tools. The framework and commercial-off-the-shelf (COTS) tool environments will enable partner agencies to share requirements and design information, deliver enhanced capability and retain institutional knowledge.

Electronic Version at: http://www.asmg-ltd.com
IEF Policy Life Cycle

- Drive by business/operational requirements contained in:
  - Legislation /International Agreements
  - Regulation
  - Agency Policy
  - Memorandum of Understanding
  - Service Level Agreements
  - Operating Procedures

- Process & architecture alignment provides data (/metadata) to enable:
  - Modeling & simulation
  - Pre-Mission Analysis and Testing
    - Identification of policy inconsistencies
    - Identification policy gaps
    - Design /Conformance / Certification Audit
  - Post mission analysis
    - Forensic Operation Audit
    - Forensic Security Audit
  - Governance

- Promotes Agile policy development
- Promotes the development of Mission Patterns & Reuse
- Promotes the retention of institutional Memory
Generic Technology Stack

Governance

Policy

Operating Procedures

Information Visualization

Information Applications & Services

Voice

Architecture

Stakeholder Requirements

ISS Policy Models

Security

ICAM, Cryptographic Services, and Logging Services

Data Dissemination Services

File Share
Email
Instant Messaging
Structured Messaging
Web Services

Data Management

User Data

Platform

Networks

Communications

Data

Management

Dissemination
Services

File Share
Email
Instant Messaging
Structured Messaging
Web Services

User Data
• **InformationSharingSpecification (Contract):** Specifies the information elements shared as part of a specific information sharing agreement and the information dissemination services to be used. A specialization of an “OperationalExchange” it specifies an agreement between two or more parties to exchange information. The Contract forms an ontological commitment between parties in a community of interest (CoI) or Community of Practice (CoP). The contract is also used to realize the information exchange requirements of either a needline or a community of interest.

• **SemanticElement:** Composite of rules governing the assembly of data elements in accordance with commitments defined by an information exchange agreement and policies pertaining to the safeguarding of sensitive information. Derived from SOPES IEDM V1: Semantic

• **TransactionalElement:** Specifies a reusable pattern comprising rules governing the assembly and processing of data and information elements. Derived from SOPES IEDM V1: Transactional

• **WrapperElement:** An attribute assigned to a WrapperElement. Source: derived from UPDM.

• **SemanticAttribute:** An attribute assigned to a semantic element. Derived from UPDM

• **TransactionalAttribute:** An attribute assigned to a TransactionalElement. Derived from UPDM

• **WrapperAttribute:** An attribute assigned to a WrapperElement. Source: derived from UPDM

• **FilteredSemanticElement:** Specifies rules for the assignment of one or more DynamicFilters to a specified SemanticElement. Source: Derived from SOPES IEDM V1

• **FilteredTransactionalElement:** Rules specifying the WrapperAttributes that are filterable at runtime.

• **FilterRule:** A rule or rules governing the inclusion of or rejection of a data or information elements based on the value of a specified attribute, or values of specified attributes.

• **Identifier:** Identifies the element (TransactionalElement or WrapperElement) that holds a unique identifier or key needed for the construction of a data set. This subtended class would contain, as a minimum, the base global unique identifier (e.g., database key, foreign keys or unique identifier) that would differentiate which Transactional or Wrapper instance (information element instances) is included in the construction of the composite. (e.g., foreign key relationships) There exists one and only one identifier for each SemanticElement or TransactionalElement.

Source: Derived from UML Profile for DODAF and MODAF (UPDM) V2.0, formal/2012-01-03 and Shared Operational Picture Exchange Services (SOPES) Information Exchange Data Model (IEDM) Version 1.0, formal/2011-05-04
3 versions of an Information Exchange Specification

1..* Filtered can be assigned to a single specification

1..1 Information Specification – it forms a pattern that can be used may reused under multiple IES. IES using different communication channels, protocols, ...,
Example of a dynamic filter used to constrain a dataset comprising all organization units in the database: (Organization_SA). During the demonstration the dynamic filters are configured using the following attributes:

- object-type-name-text is set to "NAVY"
- cat-code is set to "UNIT"

This filter would constrain the assembly of data to "Navy Units".

The two attributes needed WrapperElements are enclosed by TransactionalElement "Organization_Item_Type";

Two filters are required to set a Unit and Organizations constraint on Organization_SA SemanticElement to configure it to report only Navy Units.

The WrapperElements and WrapperAttributes depicted in this figure were defined as part of the SOPES IEDM Specification.

- Used to identify which enclosed parameters may be used to set a filter at runtime for the referenced SemanticElement
- In this example, policies for two (2) filters are being configured
- The use of Dynamic Filters will be demonstrated to reconfigure an ISE during the demonstration.
A Semantic Element identifies the Transactional Elements (data patterns) that specify the rules that govern the assembly of data and information elements needed to fulfill IES requirements.

When executed it results in the assembles for a sets of data that is complete and meaningful to other IES participants.

If defined correctly, it generates a set of data that conveys meaning among disparate information systems (e.g., situational awareness and decision support) operating within the community.

Each of the TransactionalElement used in the diagram are fully documented in the SOPES IEDM Specification (www.omg.org/spec/SOPES). The SOPES IEDM model defined a common set of assembly and processing patterns for the JC3IEMD, the data model for this example.
Adding Static Filters

- Used to identify which enclosed parameters may be used to set a filter at runtime for the referenced SemanticElement
- In this example, policies for two (2) filters are being configured
- The use of Dynamic Filters will be demonstrated to reconfigure an ISE during the demonstration.

```java
class Organisation_SA - static filter
«TransactionalElement»
SOPES::Organisation_Item _Type
+ org-item-type-typeName :string
  self.cat-code = UNIT
  self.organizationTypeName = "NAVY"

Example::Organization_SA_F
  - organizationTypeName :string
    - org-stat-oper-stat-code :char
    - org-status-orgName :char
    - reportedDataTime :char

Illustration of Attribution with a name change: obj-item-type-typeName to organizationTypeName.

The model uses name-based attribution for the rest of the subtended attributes. All attributes in the owned by the subtended TransactionalElements are integrated into the SemanticElement (Organization_SA) - maintaining the same name as in the TransactionalElement. The have been hidden to simplify the diagram.
```
• A Semantic Element can be extended using static filters (context qualifiers in the aggregation arcs) and transforms on the subtended transactional elements.

• Sensitivity marks can be added to the dataset using data transformations (operations). In the case “Report Sensitivity” is computed from the “org-item-type-typeName”, “org-stat-oper-stat-code” and “reportedDateTime”.
These Transactional Elements were extracted from the OMG Shared Operational Picture Exchange Services (SOPES) Specification, Representing a set of exchange patterns for the NATO JC3I EDM (STANAG 5525)
Simple mapping of the Wrapper Element to the Physical Table in the target Database