Introduction to Data Centric Security (DCS)

Architecture Approach to
Policy-driven Data-centric Information Sharing and Safeguarding

June 2019

Overview

- The target of the Data Centric Security (DCS) at CWIX
  - NATO has the same requirements as an collaborating group of partner agencies
- Overview of Modeling ISS Policy
- The Elements of the Proposed DCS solution for CWIX
- Questions

The Information Sharing and Safeguarding Challenge?

“At the heart of information sharing and safeguarding there lies a paradox”

Information is valuable only if it can be shared with, and used by authorized decision makers

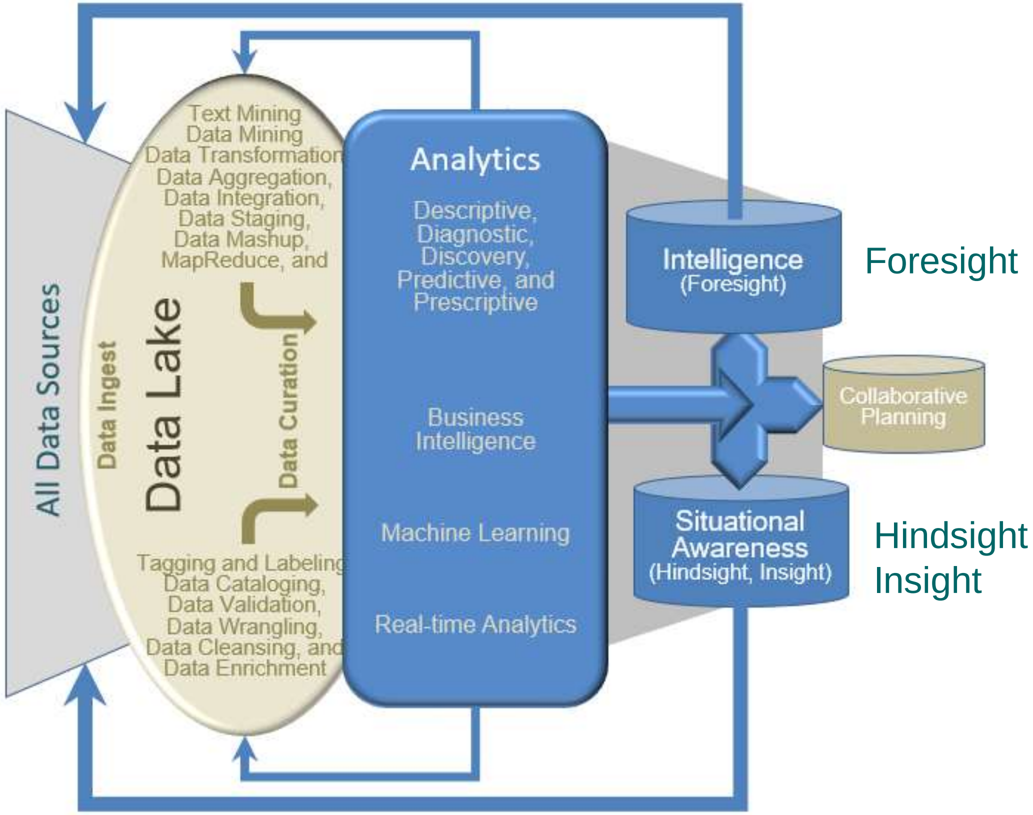
And by increasing the amount information shared, the risk of compromise also increases

- This paradox exists in every domain where sensitive (Private, Confidential, Legally-Significant or classified) information is gathered, processed, used and shared
- While sharing and safeguarding priorities and concerns appear to be mutually exclusive; in reality they are mutually reinforcing concepts:
  - Mechanisms that strengthen protection for sensitive information elements help to build **TRUST** within and between communities
  - Increased **TRUST** increases the willingness to share
- Achieving an effective balance between Sharing and Safeguarding:
  - Requires flexible, agile and adaptive mechanisms and controls during design, implementation, testing, deployment, operations and auditing
  - Represents a data/information management versus technology deficit
  - Cannot be delivered by a single organization, agency or technology

Data Usage: Data Collection, processing and Analysis

The ability to gather all-source data and create quality information for decision makers is the primary role of IM/IT

- Data is collected from all available sources, and:
- Data is tagged, labeled and catalogued to facilitate discovery, processing, sharing and safeguarding.
- Data is curated and transformed to reflect institutional standards that enables and facilitates analytics
- Data is staged for analytics, business intelligence, and machine learning …
- Analytics is performed in order to inform situational awareness (hindsight and insight), intelligence (foresight), and planning



Information Sharing and Safeguarding (ISS)

Why Share Data/Information

- Inform Decisions
  - Shared Situational Awareness (Hindsight, Insight);
  - Shared Intelligence (Foresight)
- Enable Collaboration Planning / Collective Action
- Improve Operational Posture – higher quality information:
  - (Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable, Understandable, Reliable, …, Trusted)
- Resource Multiplier
  - enable and automated response
  - Better allocation available resources

Information is only valuable or useful if it can be shared

- Data must be packaged (aggregated, transformed, marked, redacted and formatted) to balance user need and institutional security policy, assuring:
  - The quality of the information (Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable / Understandable, Reliable, …, Trusted)
  - The protection of sensitive (private, confidential, legally-significant and classified) data
- Data and information elements must be tagged and labeled, to and facilitate discovery, processing, sharing and safeguarding

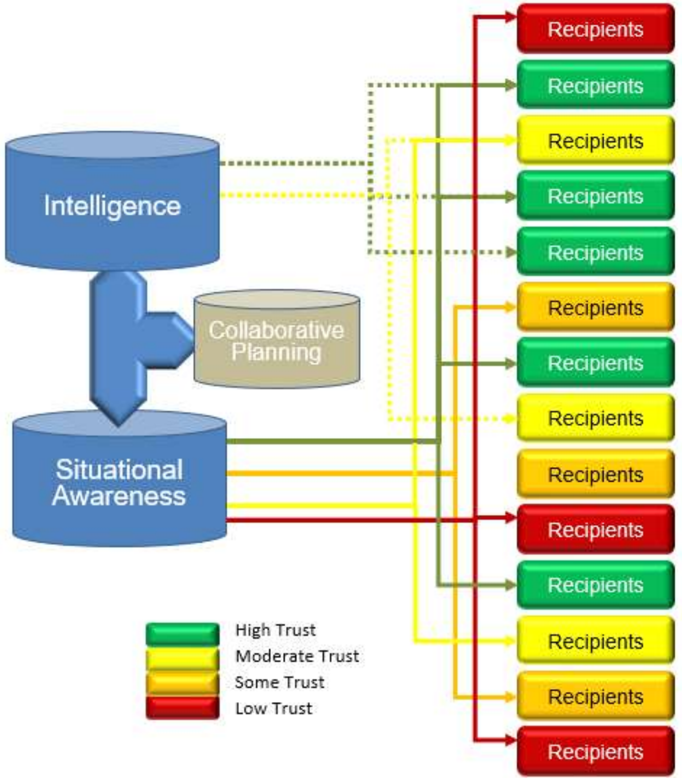
Responsible Information Sharing

Maximize the availability of quality information to authorized users, in accordance with legislation, regulation and policy, while protecting sensitive (*private, confidential, legally-significant and classified*) data from unauthorized access, release, or manipulation”

Data Sharing and Safeguarding

- Assuring that all information sharing agreements are fulfilled is a complex task
- No good plan / architecture survives for ISS will survive first contact with the operational environment
  - The legislation, regulation, ISAs, MOUs, …, and operating procedures directing information to be shared are not written in a manner that easily translates into interface design
  - legislation, regulation, ISAs, MOUs, …, and operating procedures must be applied to each dataset separately
  - Information sharing and security policies contradict each other
  - It is unlikely that the data/information needs of each internal or external recipient are well understood
  - Requirement for data/information are in a constant state of flux
- Tradition interface (API) design and maintenance approaches cannot keep pace

The ability to share information in a responsible and trusted manner is the cornerstone of a digital strategy



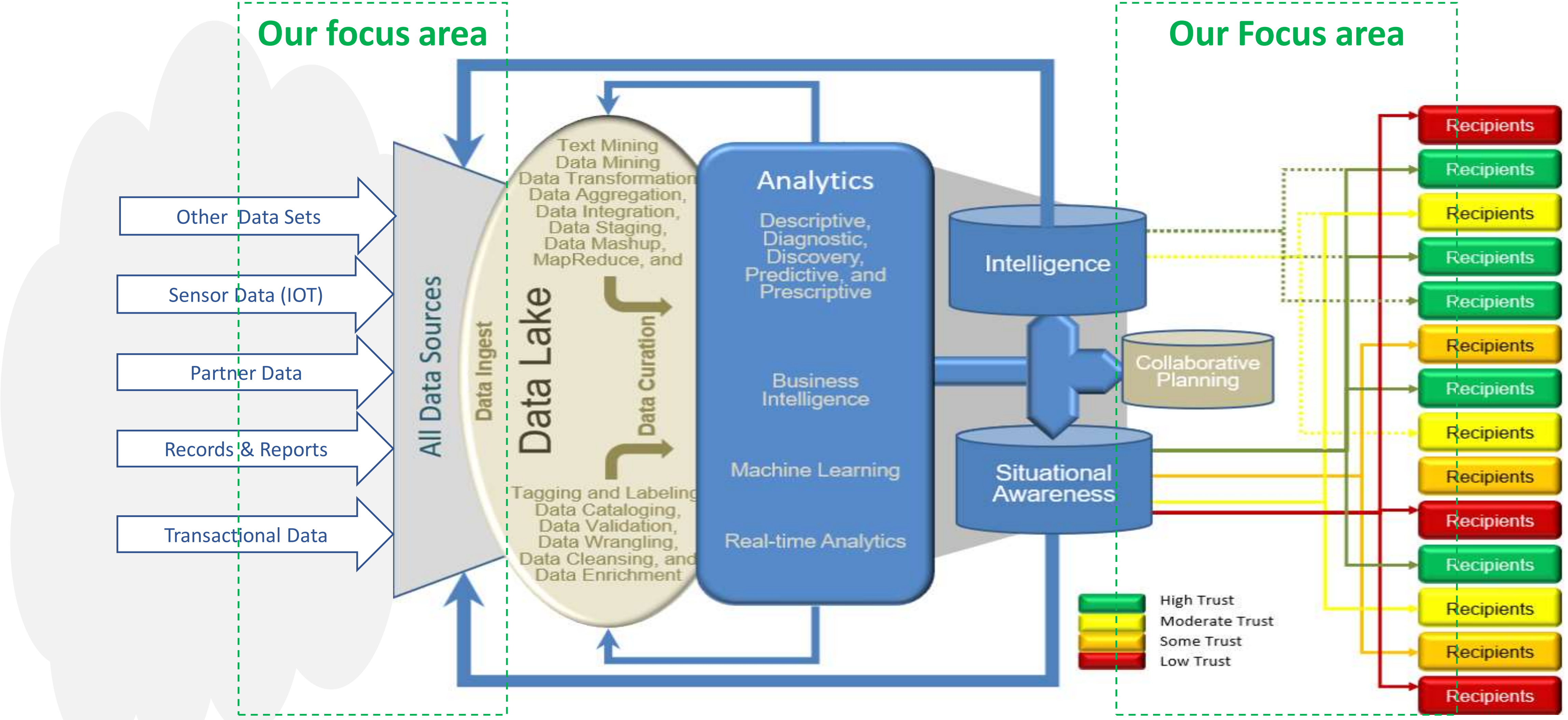
Responsible Sharing

Maximizing the sharing and availability of information of information, while simultaneously protecting sensitive (private, confidential, legally-significant and classified) information from unauthorized access, use, release, or manipulation.

Quality Information

Provision of information that is Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable / Understandable, Reliable, Trusted, **etc …**

Modern Information Management on a slide



Our focus area

Our Focus area

Other Data Sets

Sensor Data (IOT)

Partner Data

Records & Reports

Transactional Data

All Data Sources

Data Ingest

Data Lake

Text Mining
Data Mining
Data Transformation
Data Aggregation,
Data Integration,
Data Staging,
Data Mashup,
MapReduce, and

Data Curation

Tagging and Labeling
Data Cataloging,
Data Validation,
Data Wrangling,
Data Cleansing, and
Data Enrichment

Analytics

Descriptive,
Diagnostic,
Discovery,
Predictive, and
Prescriptive

Business
Intelligence

Machine Learning

Real-time Analytics

Intelligence

Collaborative
Planning

Situational
Awareness

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

Recipients

🟩 High Trust

🟨 Moderate Trust

🟧 Some Trust

🟥 Low Trust

AN OMG STANDARD IEF Information Exchange Framework™

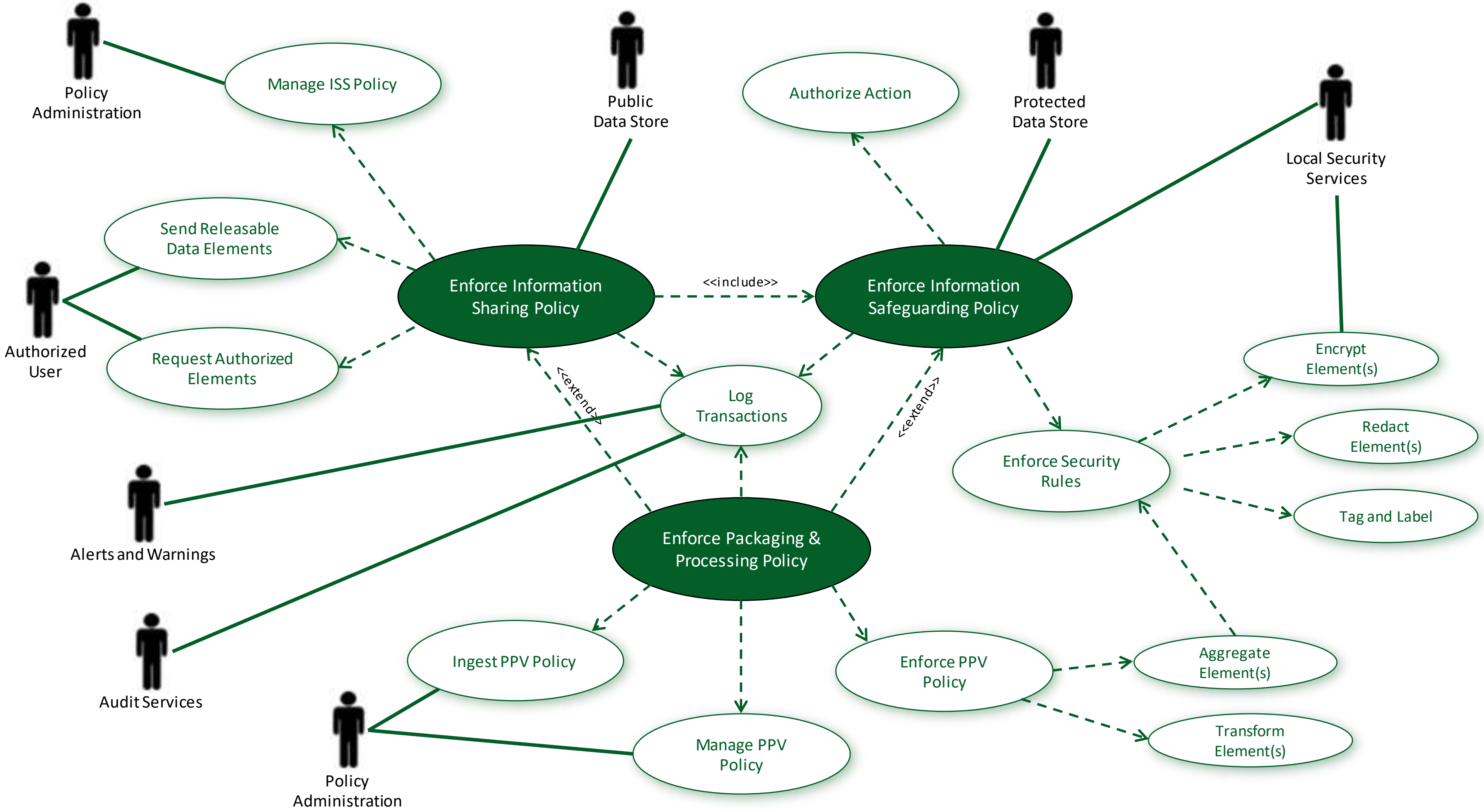
AN OMG STANDARD IEPPV Information Exchange Packaging Policy Vocabulary™

OMG OBJECT MANAGEMENT GROUP®

ASMG ADVANCED SYSTEMS MANAGEMENT GROUP

Generic Use-case for Information Sharing and Safeguarding

KYMadvisors



AN OMG STANDARD IEF Information Exchange Framework™

AN OMG STANDARD IEPPV Information Exchange Packaging Policy Vocabulary™

OMG OBJECT MANAGEMENT GROUP®

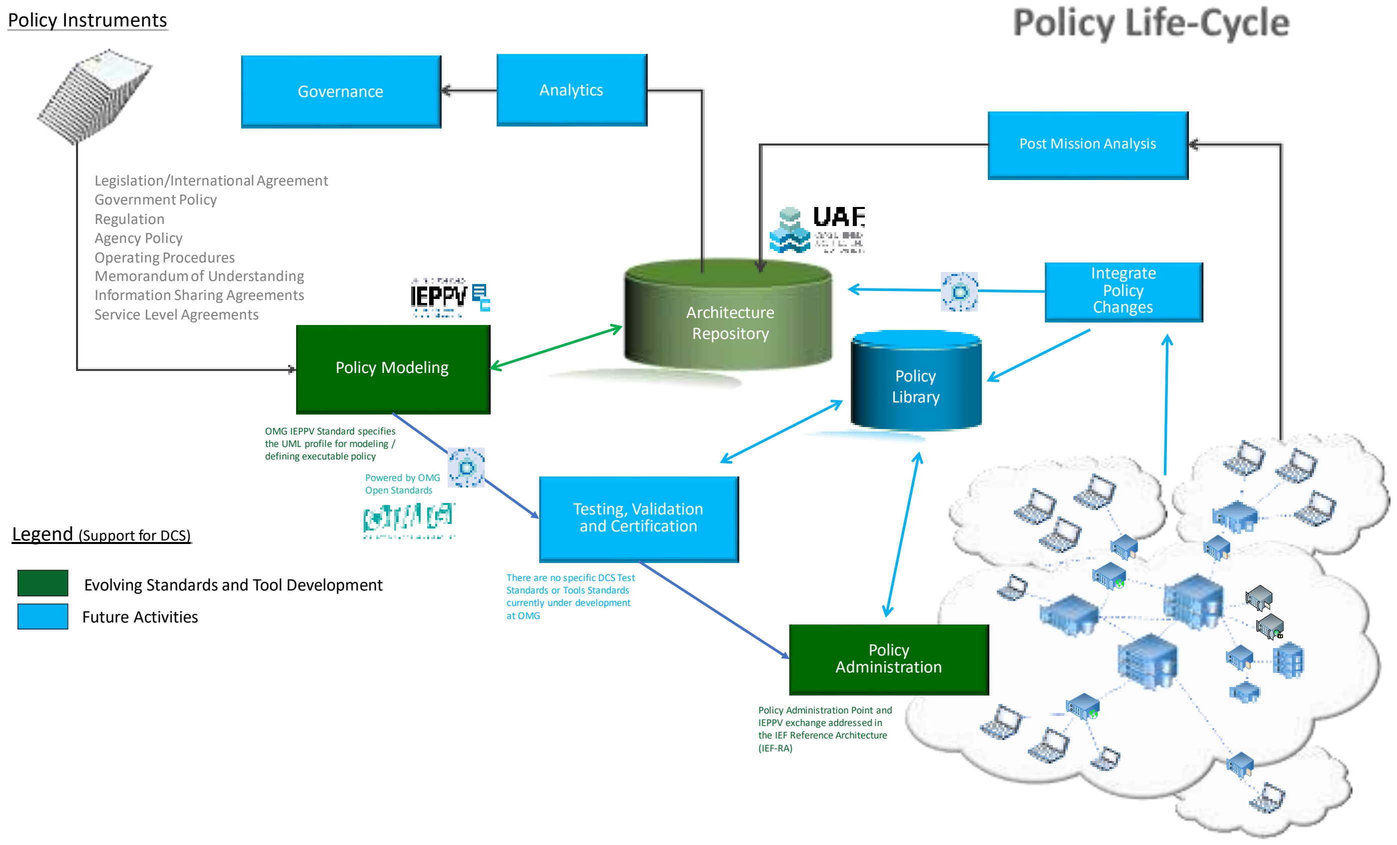
Keys to a Solutions Success

- Separate Business, IM and IT Concerns
- Augment and not replace user applications and infrastructure
- Increase flexibility, adaptability and agility during development and operations
  - Model driven architecture / Use of MBSE
  - Rule-based applications / Separate business rules from the code
  - Separate life-cycle for business rules and software
  - Run load of business rules
  - Runtime administration of rules (increased flexibility, adaptability and agility)
- Enhanced logging and auditing
  - Demonstrate responsible, Trusted and Auditable ISS
  - Enable real-time monitoring
  - Enable forensic Auditing
- Integration of open standards

Policy Life-cycle – Separating Concerns

Policy, Applications and IT have separate life-cycles

- Networks and Platforms can be deployed independent of applications (e.g., Cloud, On-prem, Hybrid)
- Application are developed to enforce policies (rules and constraints) based on standardized policy models and rapidly deployed to deployed infrastructure
- Policies are defined by the business - based on user / business / operational needs - and deployed to the applications as data sets that are ingested at runtime.
- Libraries of policy models can be maintained and deployed as needed



OMG IEPPV Standard specifies the UML profile for modeling / defining executable policy

Powered by OMG Open Standards

There are no specific DCS Test Standards or Tools Standards currently under development at OMG

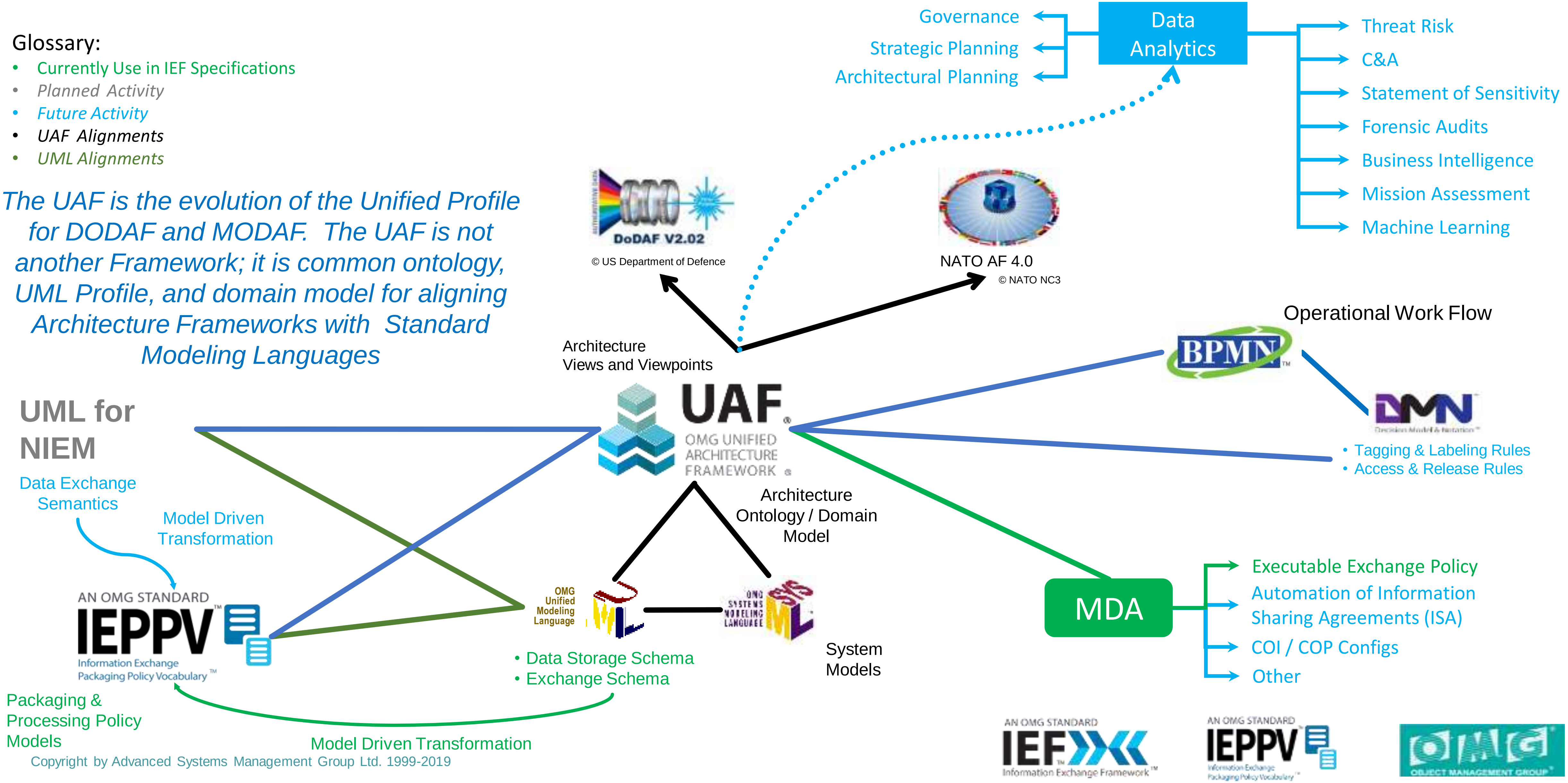
Policy Administration Point and IEPPV exchange addressed in the IEF Reference Architecture (IEF-RA)

Architecting Policy and ISS Capability for the Business

Glossary:

- Currently Use in IEF Specifications
- *Planned Activity*
- *Future Activity*
- *UAF Alignments*
- *UML Alignments*

The UAF is the evolution of the Unified Profile for DODAF and MODAF. The UAF is not another Framework; it is common ontology, UML Profile, and domain model for aligning Architecture Frameworks with Standard Modeling Languages



Data Analytics

Governance

Strategic Planning

Architectural Planning

Threat Risk

C&A

Statement of Sensitivity

Forensic Audits

Business Intelligence

Mission Assessment

Machine Learning

© US Department of Defence

NATO AF 4.0

© NATO NC3

Architecture Views and Viewpoints

Operational Work Flow

- Tagging & Labeling Rules
- Access & Release Rules

UML for NIEM

Data Exchange Semantics

Model Driven Transformation

Architecture Ontology / Domain Model

System Models

- Data Storage Schema
- Exchange Schema

MDA

Executable Exchange Policy

Automation of Information Sharing Agreements (ISA)

COI / COP Configs

Other

Packaging & Processing Policy Models

Model Driven Transformation

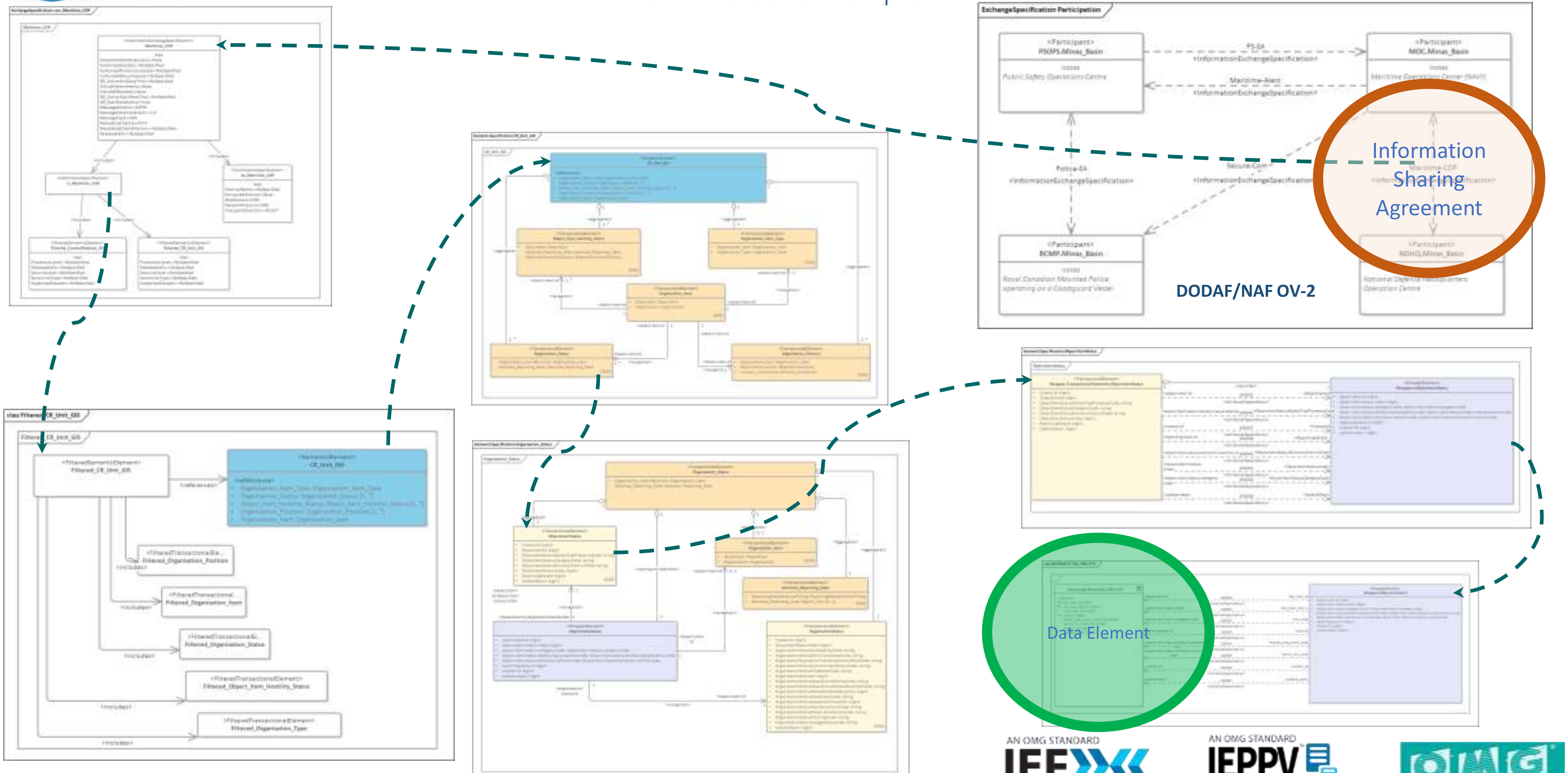
ASMG
ADVANCED SYSTEMS MANAGEMENT GROUP
KYMadvisors
DoDAF V2.02
BPMN
DMN
Decision Model & Notation
UAF
OMG UNIFIED ARCHITECTURE FRAMEWORK
OMG Unified Modeling Language
OMG SYSTEMS MODELING LANGUAGE
AN OMG STANDARD
IEPPV
Information Exchange Packaging Policy Vocabulary
AN OMG STANDARD
IEF
Information Exchange Framework
AN OMG STANDARD
IEPPV
Information Exchange Packaging Policy Vocabulary
OMG
OBJECT MANAGEMENT GROUP

ASMG ADVANCED SYSTEMS MANAGEMENT GROUP

KYMadvisors

Full Traceability ISA to Data Element

STANAG 5525 Example



ExchangeSpecification Participation
«Participant» PSOPS.Minas_Basin
Public Safety Operations Centre
«Participant» MOC.Minas_Basin
Maritime Operations Center (NAVY)
«Participant» RCMP.Minas_Basin
Royal Canadian Mounted Police operating on a Coastguard Vessel
«Participant» NDHQ.Minas_Basin
National Defence Headquarters Operation Centre
PS-SA
Maritime-Alert
Police-SA
Secure-Com
Maritime-COP
«InformationExchangeSpecification»
Information Sharing Agreement
DODAF/NAF OV-2
class Filtered_CB_Unit_GIS
«FilteredElement» Filtered_CB_Unit_GIS
CB_Unit_GIS
Filtered_Organisation_Position
Filtered_Organisation_Item
Filtered_Organisation_Status
Filtered_Object_Item_Hostility_Status
Filtered_Organisation_Type
«includes»
Data Element

AN OMG STANDARD IEF Information Exchange Framework™

AN OMG STANDARD IEPPV Information Exchange Packaging Policy Vocabulary™

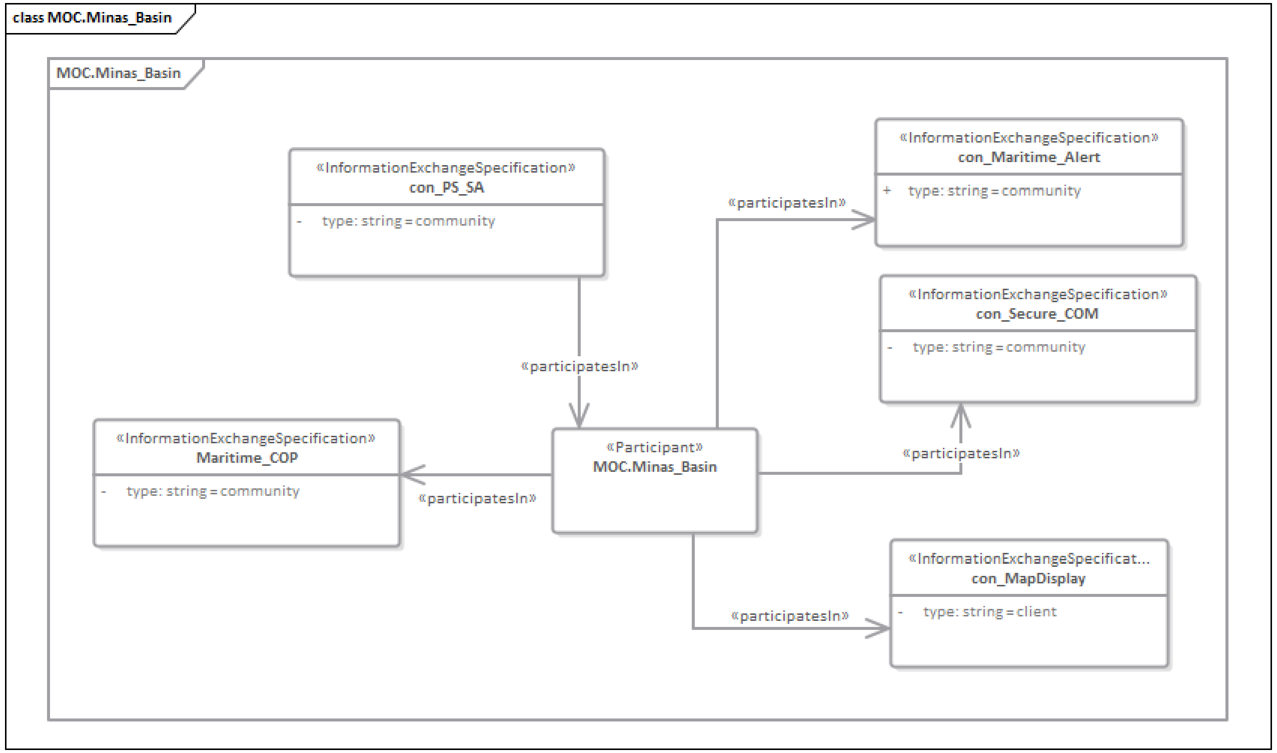
OMG OBJECT MANAGEMENT GROUP®

Participation Models

- Identify the specific participation of a partner in the Information Sharing Agreements, CoIs, …

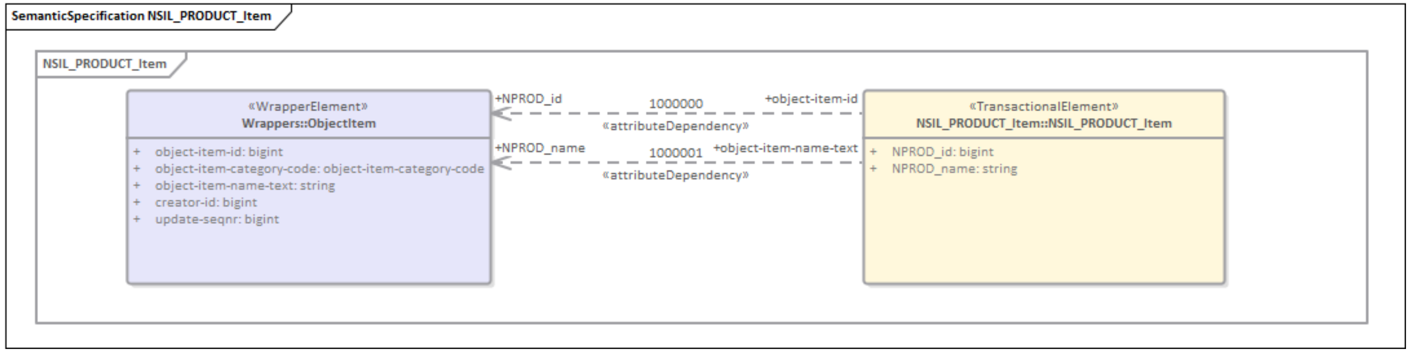
- Reduces complexity of diagrams for stakeholders

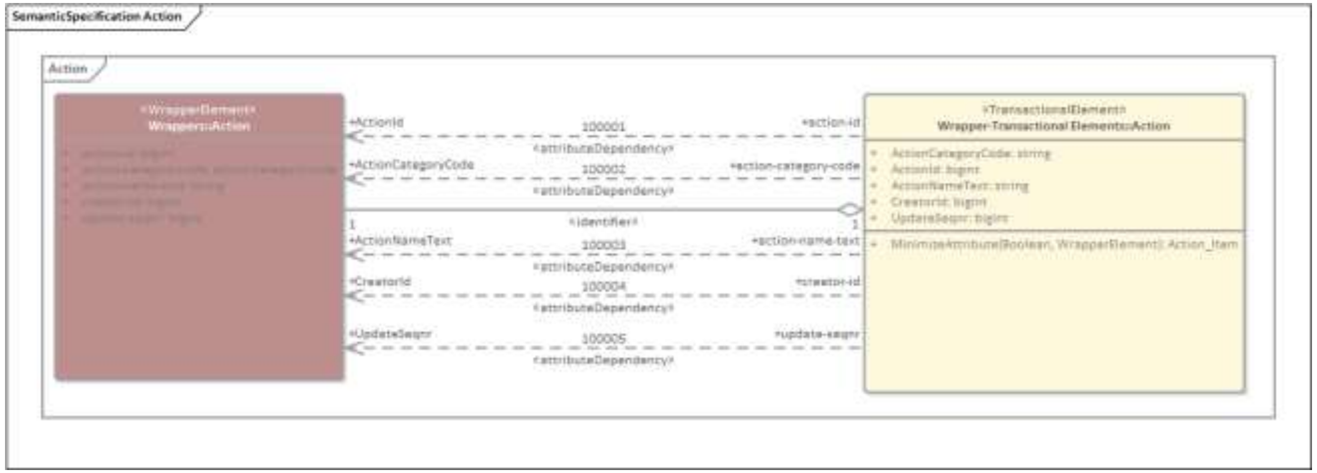
- Models can be mined to produce spreadsheets and report to aid discussion with stakeholders


class MOC.Minas_Basin
MOC.Minas_Basin
«InformationExchangeSpecification»
con_PS_SA
- type: string = community
«InformationExchangeSpecification»
con_Maritime_Alert
+ type: string = community
«InformationExchangeSpecification»
con_Secure_COM
- type: string = community
«InformationExchangeSpecification»
Maritime_COP
- type: string = community
«Participant»
MOC.Minas_Basin
«InformationExchangeSpecificat...
con_MapDisplay
- type: string = client
«participatesIn»
«participatesIn»
«participatesIn»
«participatesIn»
«participatesIn»

Redacting Data Elements

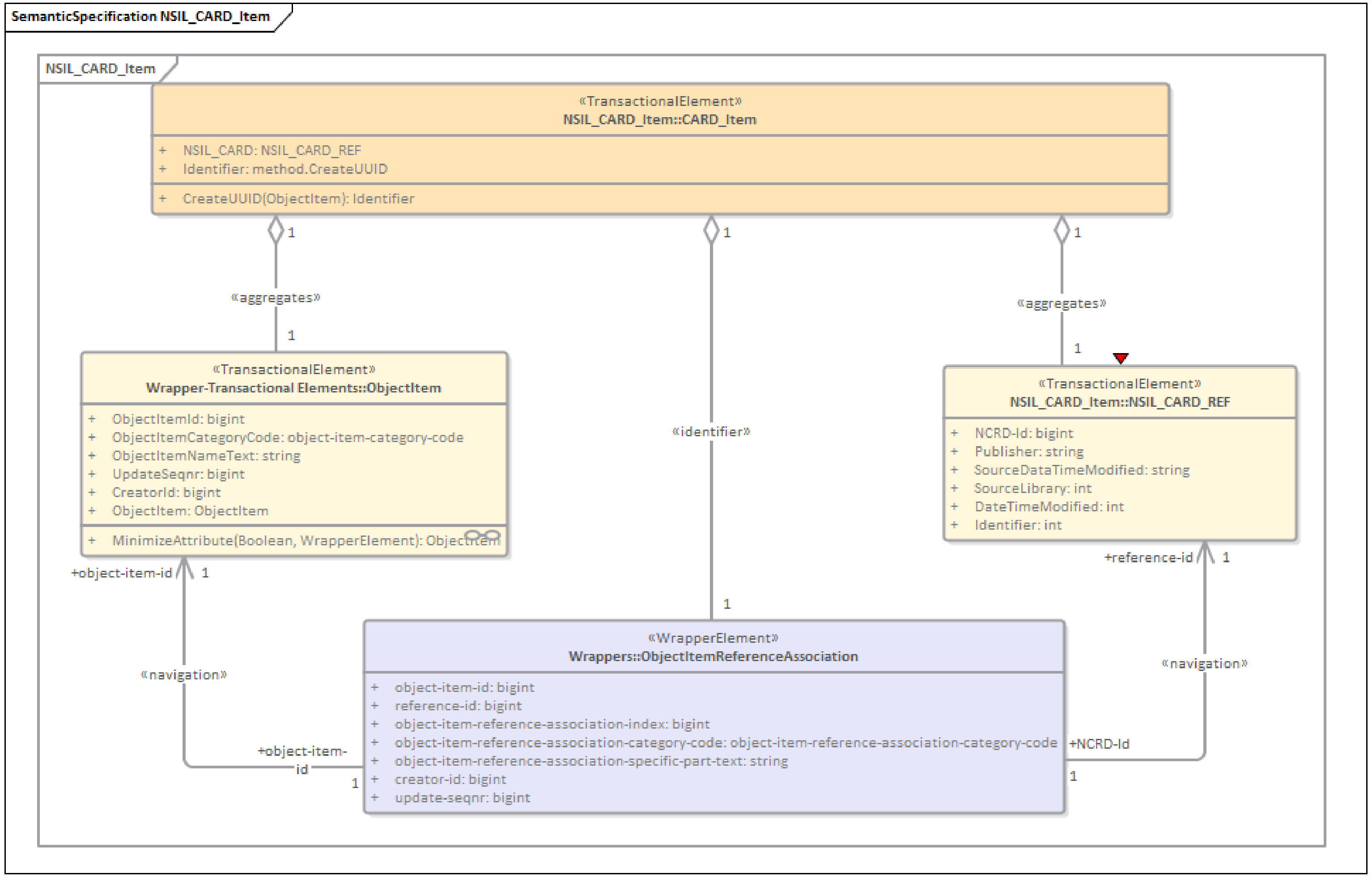
- Redact can be performed by:
    - Sub-setting the data during modeling
    - And Operation in the consuming TransactionalElement





Operations Add many Capabilities.

- Operations can be used to:
  - Transform Data
  - Redact Data
  - Tag and Label Data
  - And more



«TransactionalElement»
NSIL_CARD_Item::CARD_Item

- + NSIL_CARD: NSIL_CARD_REF
- + Identifier: method.CreateUUID
- + CreateUUID(ObjectItem): Identifier

«TransactionalElement»
Wrapper-Transactional Elements::ObjectItem

- + ObjectItemId: bigint
- + ObjectItemCategoryCode: object-item-category-code
- + ObjectItemNameText: string
- + UpdateSeqnr: bigint
- + CreatorId: bigint
- + ObjectItem: ObjectItem
- + MinimizeAttribute(Boolean, WrapperElement): ObjectItem

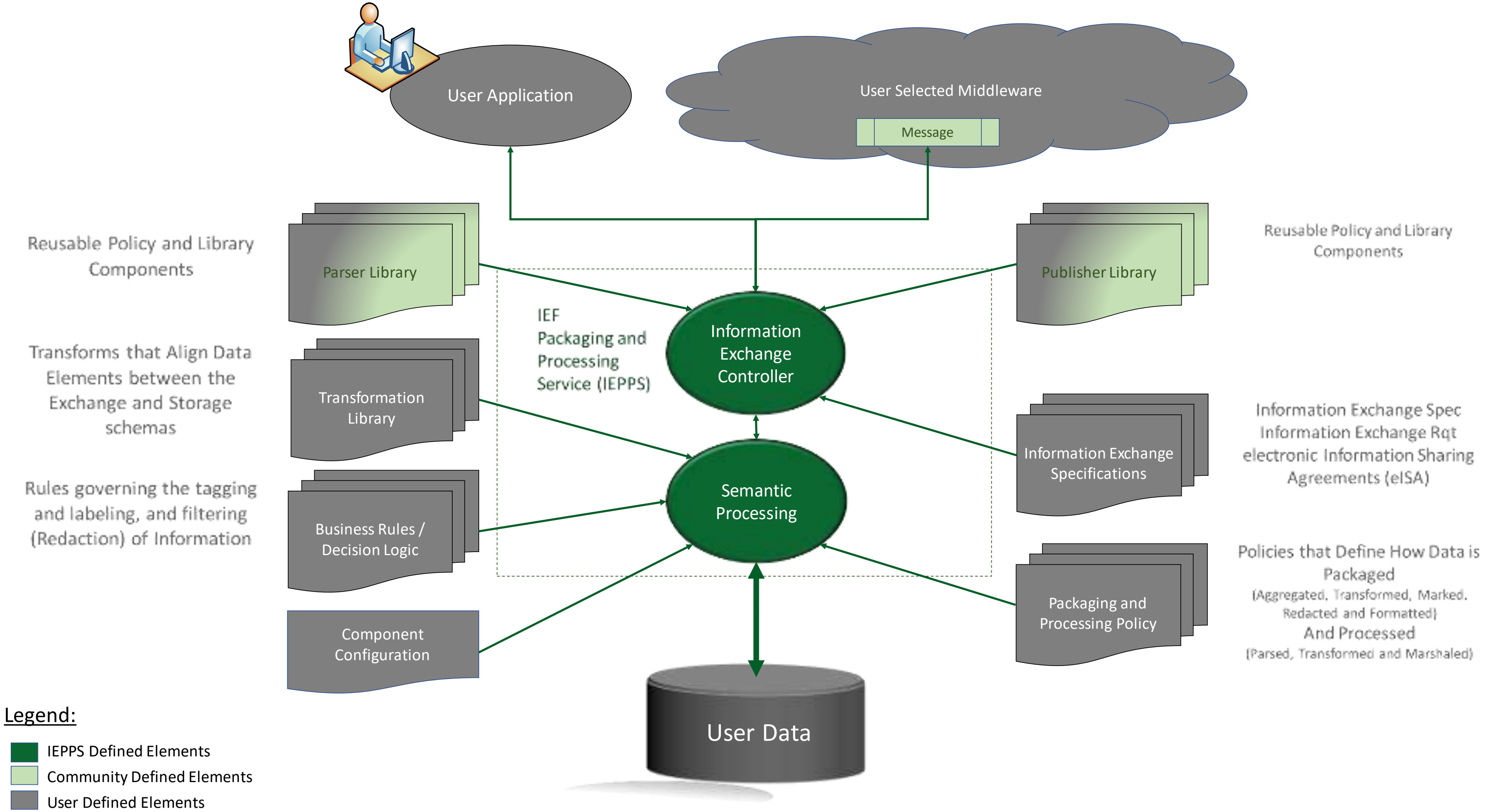
«TransactionalElement»
NSIL_CARD_Item::NSIL_CARD_REF

- + NCRD-Id: bigint
- + Publisher: string
- + SourceDataTimeModified: string
- + SourceLibrary: int
- + DateTimeModified: int
- + Identifier: int

«WrapperElement»
Wrappers::ObjectItemReferenceAssociation

- + object-item-id: bigint
- + reference-id: bigint
- + object-item-reference-association-index: bigint
- + object-item-reference-association-category-code: object-item-reference-association-category-code
- + object-item-reference-association-specific-part-text: string
- + creator-id: bigint
- + update-seqnr: bigint

Separating Policies and Rules from Enabling Technology



User Application

User Selected Middleware

Message

Reusable Policy and Library Components

Parser Library

Transforms that Align Data Elements between the Exchange and Storage schemas

Transformation Library

Rules governing the tagging and labeling, and filtering (Redaction) of Information

Business Rules / Decision Logic

Component Configuration

IEF Packaging and Processing Service (IEPPS)

Information Exchange Controller

Semantic Processing

User Data

Publisher Library

Reusable Policy and Library Components

Information Exchange Specifications

Information Exchange Spec
Information Exchange Rqt
electronic Information Sharing Agreements (eISA)

Packaging and Processing Policy

Policies that Define How Data is Packaged
(Aggregated, Transformed, Marked, Redacted and Formatted)
And Processed
(Parsed, Transformed and Marshaled)

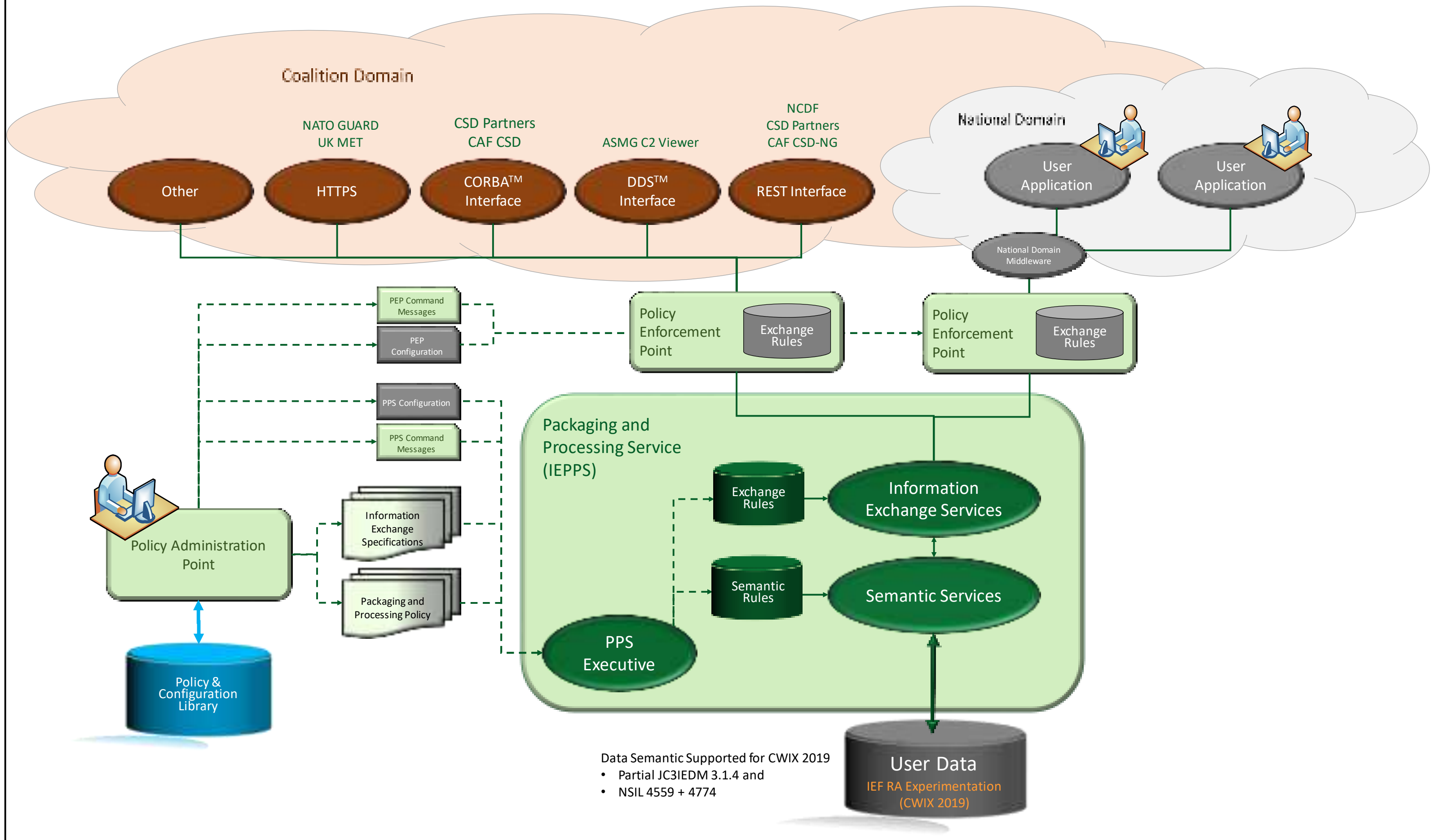
Legend:

- 🟩 IEPPS Defined Elements
- 🟩 Community Defined Elements
- ⬛ User Defined Elements

Operational Node

Common software for each node with operational needs being addressed by:

- Policies specific to their operations and data environment
- Libraries configured to their specific needs
- Confutation and rules tailored to their needs



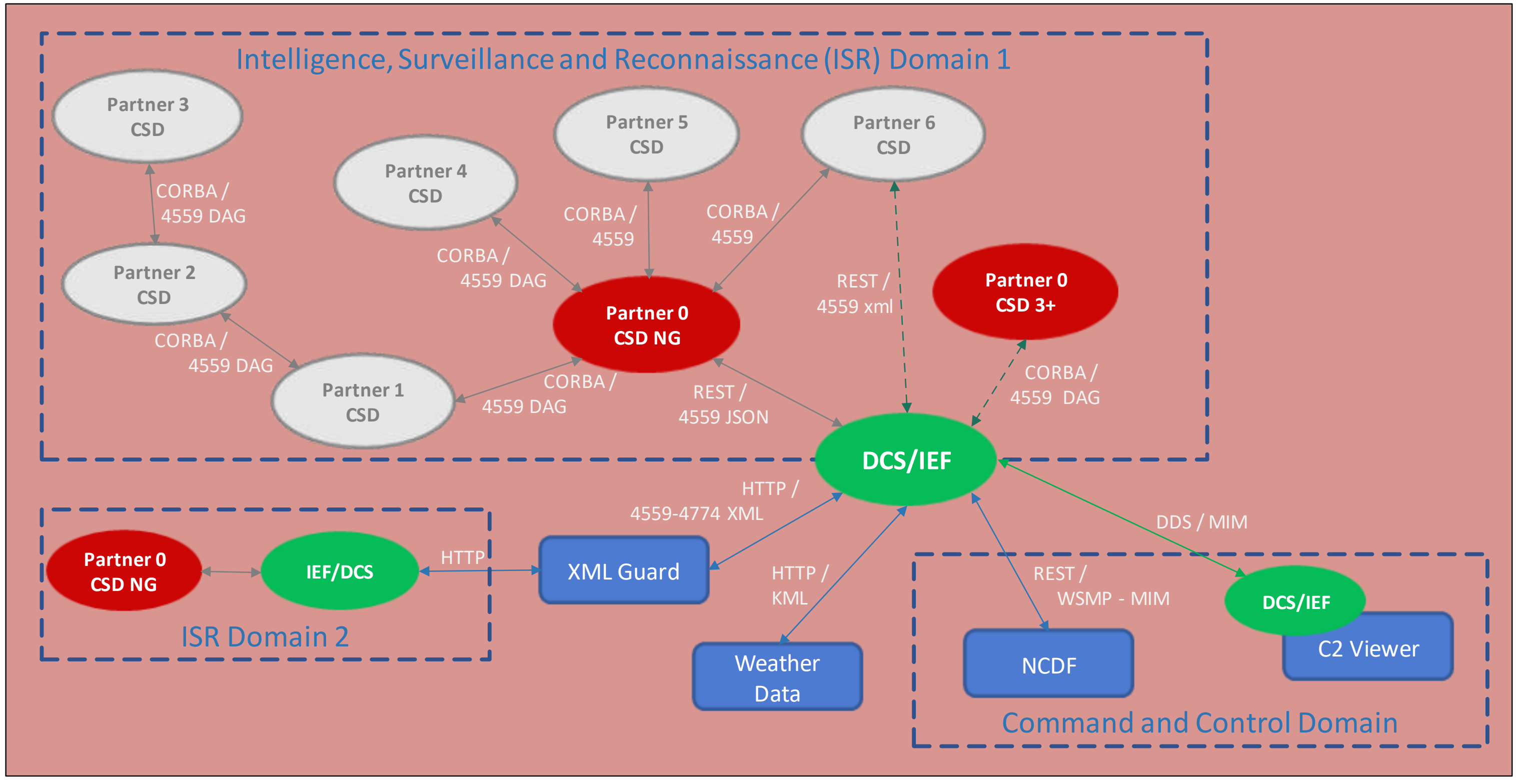
Data Semantic Supported for CWIX 2019

- Partial JC3IEDM 3.1.4 and
- NSIL 4559 + 4774

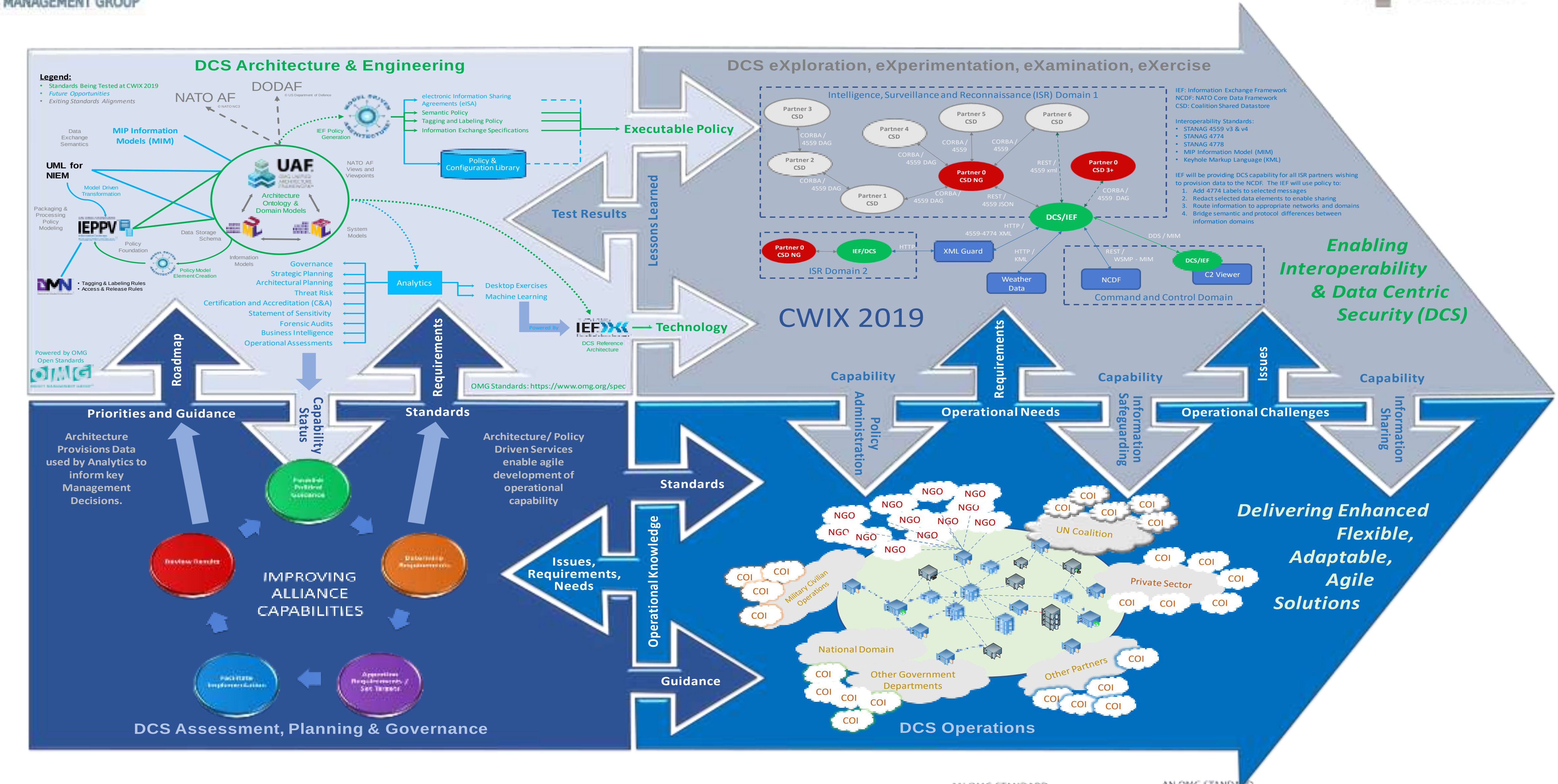
CWIX Testing and Demonstration

Testing at CWIX is seeking to verify that the proposed Architecture drive approach can be used to:

- Add DCS capability
  - Tagging and labeling (4777)
  - Selective data redaction
  - Balance the data needs and security considerations for partners at different levels of trust
- Mediate the flow of data two operational domains with differing:
  - Information semantics
  - Messaging and network protocols



Evolutionary approach to ISS Capability



DCS Architecture & Engineering

Legend:

- Standards Being Tested at CWIX 2019
- *Future Opportunities*
- *Exiting Standards Alignments*

DCS eXploration, eXperimentation, eXamination, eXercise

IEF: Information Exchange Framework
NCDF: NATO Core Data Framework
CSD: Coalition Shared Datastore

Interoperability Standards:

- STANAG 4559 v3 & v4
- STANAG 4774
- STANAG 4778
- MIP Information Model (MIM)
- Keyhole Markup Language (KML)

IEF will be providing DCS capability for all ISR partners wishing to provision data to the NCDF. The IEF will use policy to:

1. Add 4774 Labels to selected messages
2. Redact selected data elements to enable sharing
3. Route information to appropriate networks and domains
4. Bridge semantic and protocol differences between information domains

Enabling Interoperability & Data Centric Security (DCS)

DCS Assessment, Planning & Governance

Priorities and Guidance
Standards
Provide Political Guidance
Determine Requirements
Apportion Requirements / Set Targets
Facilitate Implementation
Review Results
IMPROVING ALLIANCE CAPABILITIES
Standards
Issues, Requirements, Needs
Operational Knowledge
Guidance

Architecture Provisions Data used by Analytics to inform key Management Decisions.

Architecture/ Policy Driven Services enable agile development of operational capability

DCS Operations

Delivering Enhanced Flexible, Adaptable, Agile Solutions

Mike Abramson
Advanced Systems Management Group (ASMG) Ltd.
Co-Chair C4I DTF at OMG, Co-Chair IEF WG at OMG
265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1
Phone: (613) 567-7097 x222
Email: abramson@asmg-ltd.com

Vijay Mehra
KYM Advisors
Co-Chair IEF WG at OMG
4400 Fair Lakes Ct., Suite 101A, Fairfax, VA 22033
Phone: (571) 510-0930
Email: vijay.mehra@kymadvisors.com

Back-up Slides

Information Exchange Framework (IEF)

- Standards Specifications
  - http://www.omg.org/spec/IEPPV/
  - http://www.omg.org/spec/IEF-RA/
  - IEPPS RFP was issued Dec 2017 and currently being developed