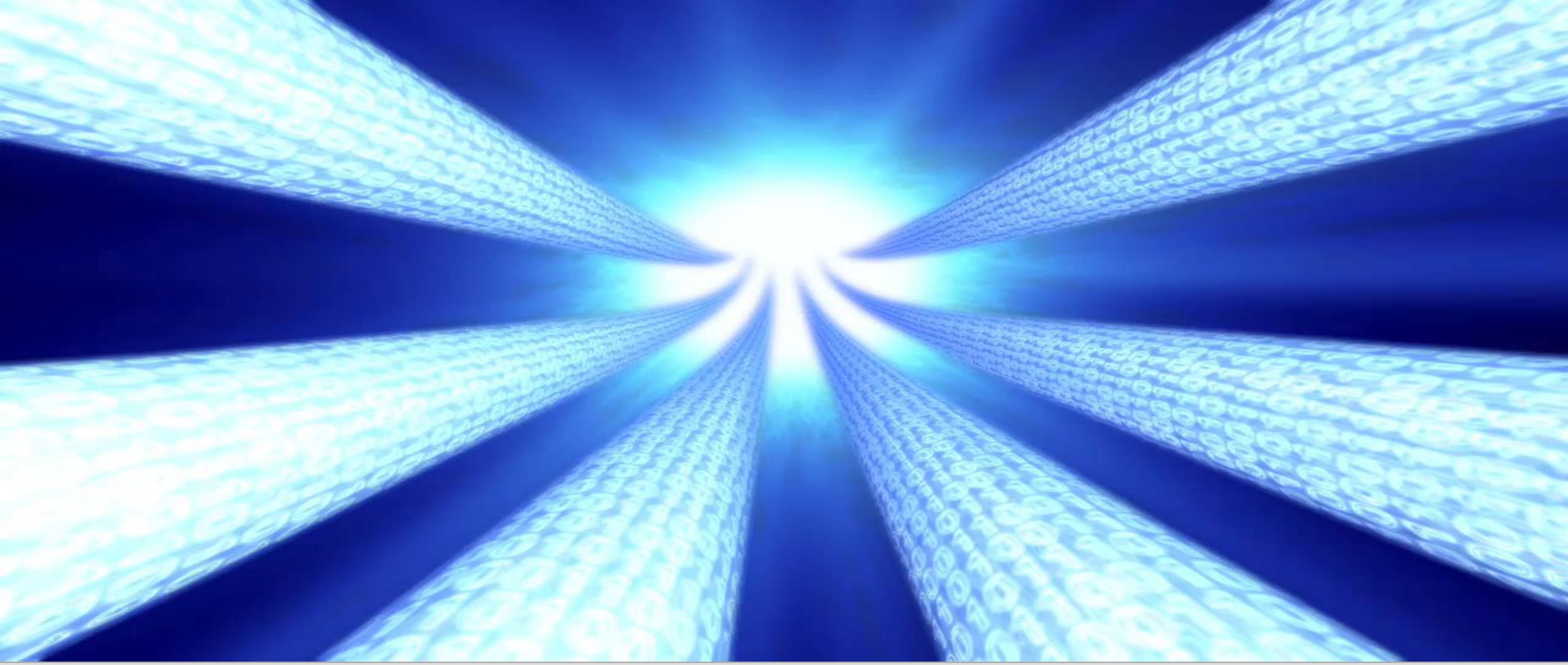
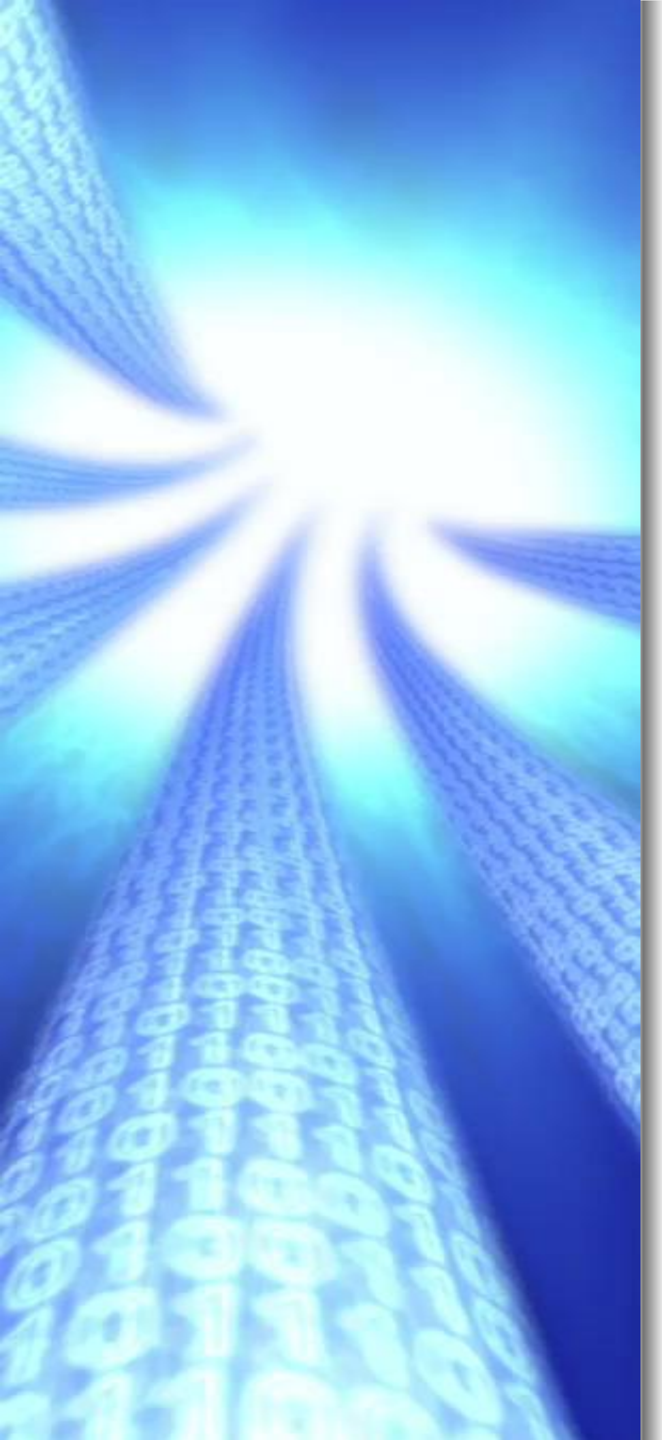


Enabling System-to-System (S2S) Information Sharing

By: Poewan Lau

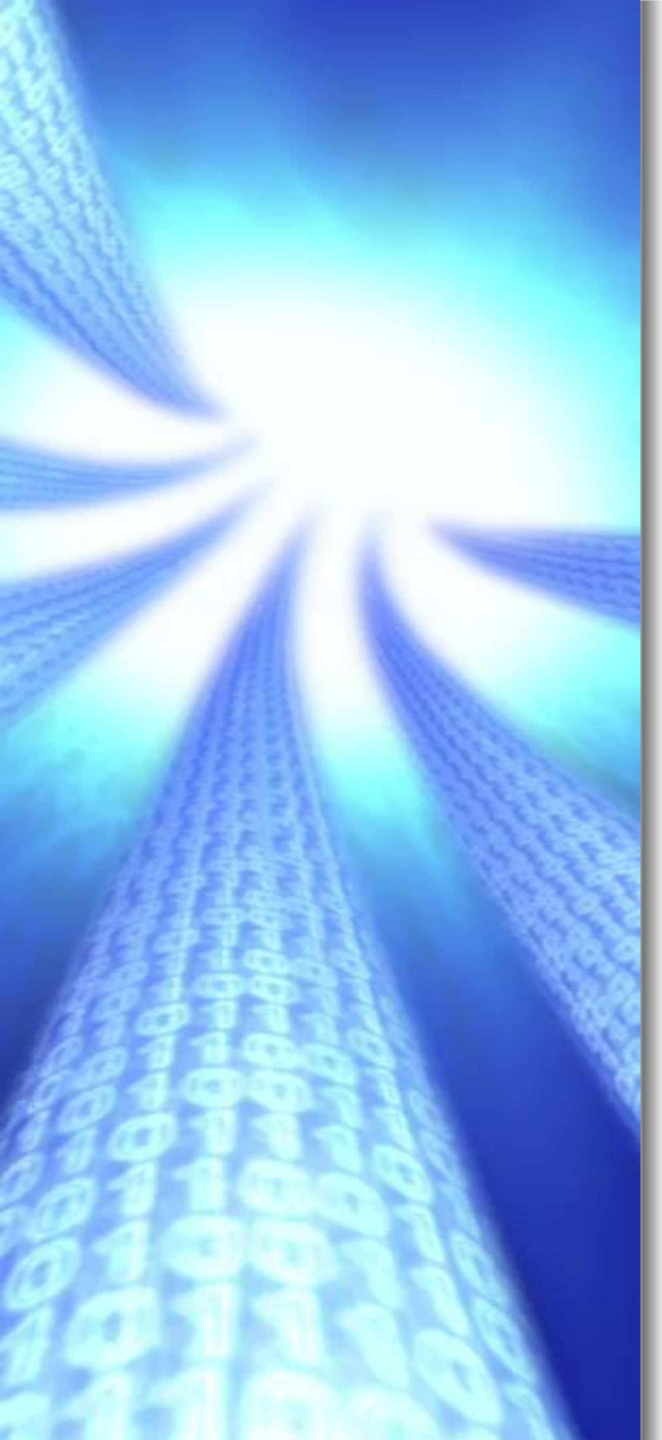


“Necessity is the Mother of Invention”

Public Sector have great and growing need to transform data into information for decision makers (e.g., National Security, Public Safety, Public Health, Emergency Management and Program Delivery)

Public Sector data sets often includes sensitive (e.g., private, confidential, legally-significant and classified) data and information elements that need to be protected

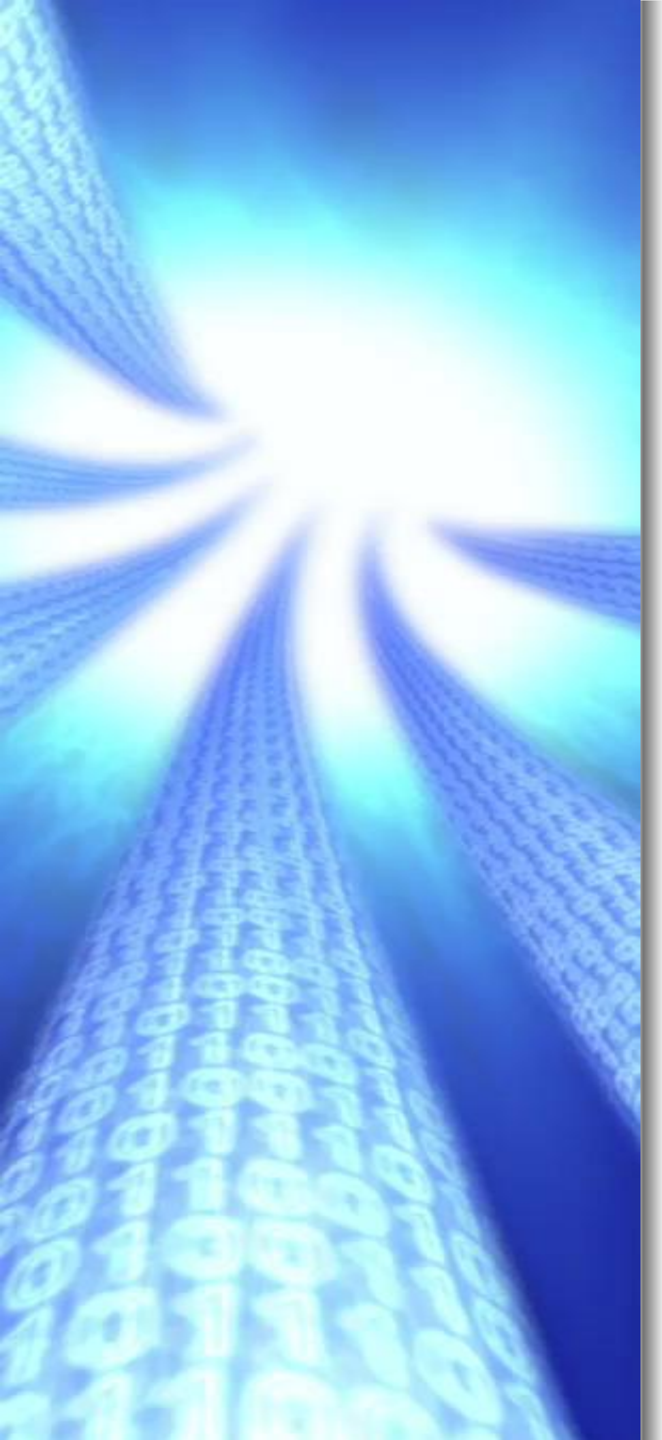
This need led to Canadian Initiatives to develop Trusted Information Exchange Services (TIES), Secure Access Management for Secure Operational Networks (SAMSON), Information Exchange Framework (IEF) and Secure Data Services (SDS).



Why Focus on Information Sharing

- Desire to use of all source data to inform decision makers by providing an infrastructure that enables scalable and secure data and information:
  - Collection
  - Processing
  - Analytics, decision aids, AI and machine learning
  - Sharing and Safeguarding
  - Visualization
- Improve the quality and availability information for decision makers
- Use Information as a Resource Multiplier
- Deliver Information Advantage

Shared Semantics



- Common community semantic specifications (e.g., NIEM, MIM and NISILI (NATO ISR)) and semantic standards will simplify the process of developing and deploying ISS solutions
  - NATO Standards xxxx, ADATP-xx and Technical Notes (TN) for coalition ISS
  - NIEM for Intergovernmental ISS
  - OASIS Standards for commercial and other data domain
- Multiple Canadian governments and agencies looking to NIEM and other specifications as a foundation for ISS
- Shared Semantics are not the whole story, Users:
  - Require common labeling and binding standards to enable security services, data processing and data discovery
  - Require common services to implement and enforce ISS policy
  - Require tools to manage and administer the ISS policy lifecycle
  - Require tools to plan and deploy ISS solutions
  - Require semantic models to address local realities (e.g., Internationalization)

The Data Security Challenge

- As data in aggregated from one or more a sources its sensitivity (privacy, confidentiality, legal-significance or classification) often increases – Restricting its release
- Rules of access and/or exchange require the application of policy based on content that changes from instance to instances (or message to message) – and rules change based on operational conditions
- An inability to assess the runtime sensitivity of data has been an impenetrable barrier to developing and delivering information interoperability (providing the right information to the right entity at the right time)
- Each instance of a data message can contain variations in content that affects access and releaseability

Traditional Strategies

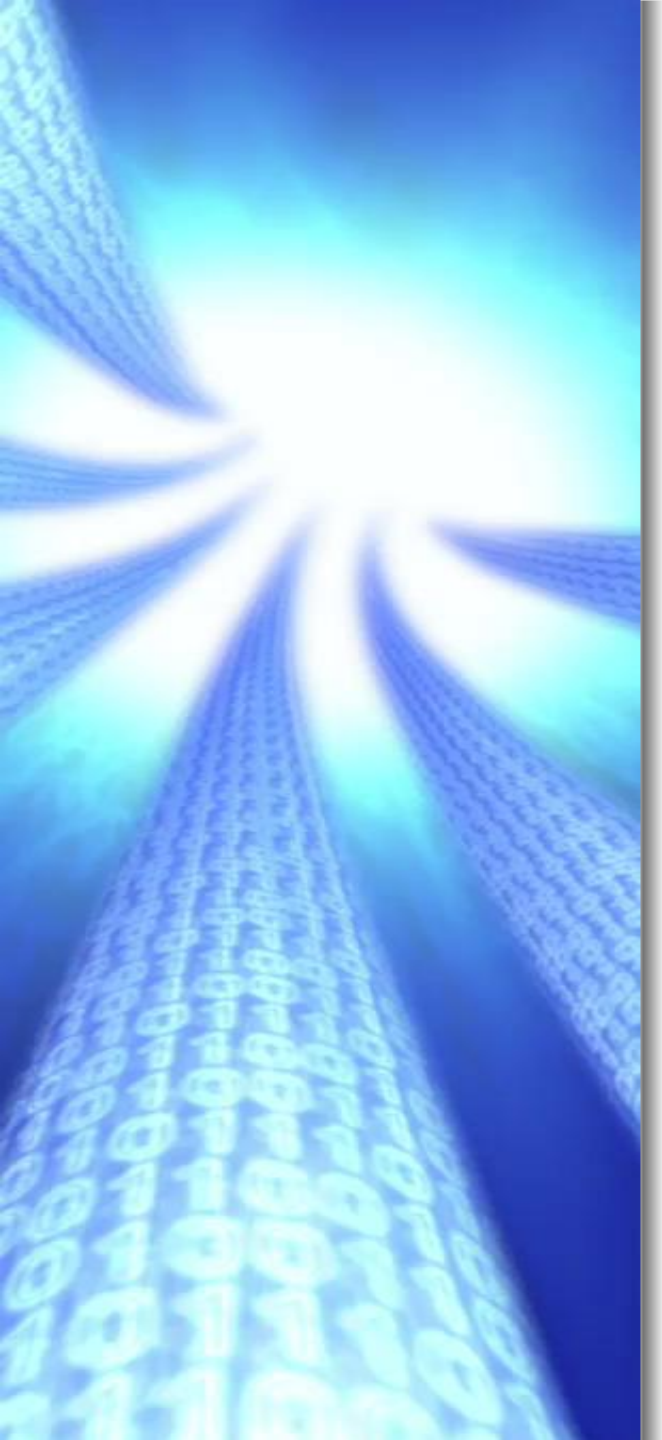
- Strategies:
  - Place a human in the loop to exercise judgement and control
  - Place a human in the loop to label the messages to enable automation of policy enforcement
- They works reasonable well when exchanging data using Email, Chat and File Share where the human is typically generating the data content
- Not so much for system-to-system (machine-to-machine) data exchange where content is automatically generated in real-time at machine speeds. humans are unable to operate at these speeds; so these method make broad-based, sustainable interoperability a bridge too far
- There is a requirement to develop services that automate the enforcement of ISS policies for the packaging and processing of information exchanges (i.e., Data Centric Security)

Sharing and Safeguarding are Necessary Mutually Reinforcing Concepts

If one can demonstrate that they can protect a data owners sensitive data

It will build trust

An the will be more likely to share information



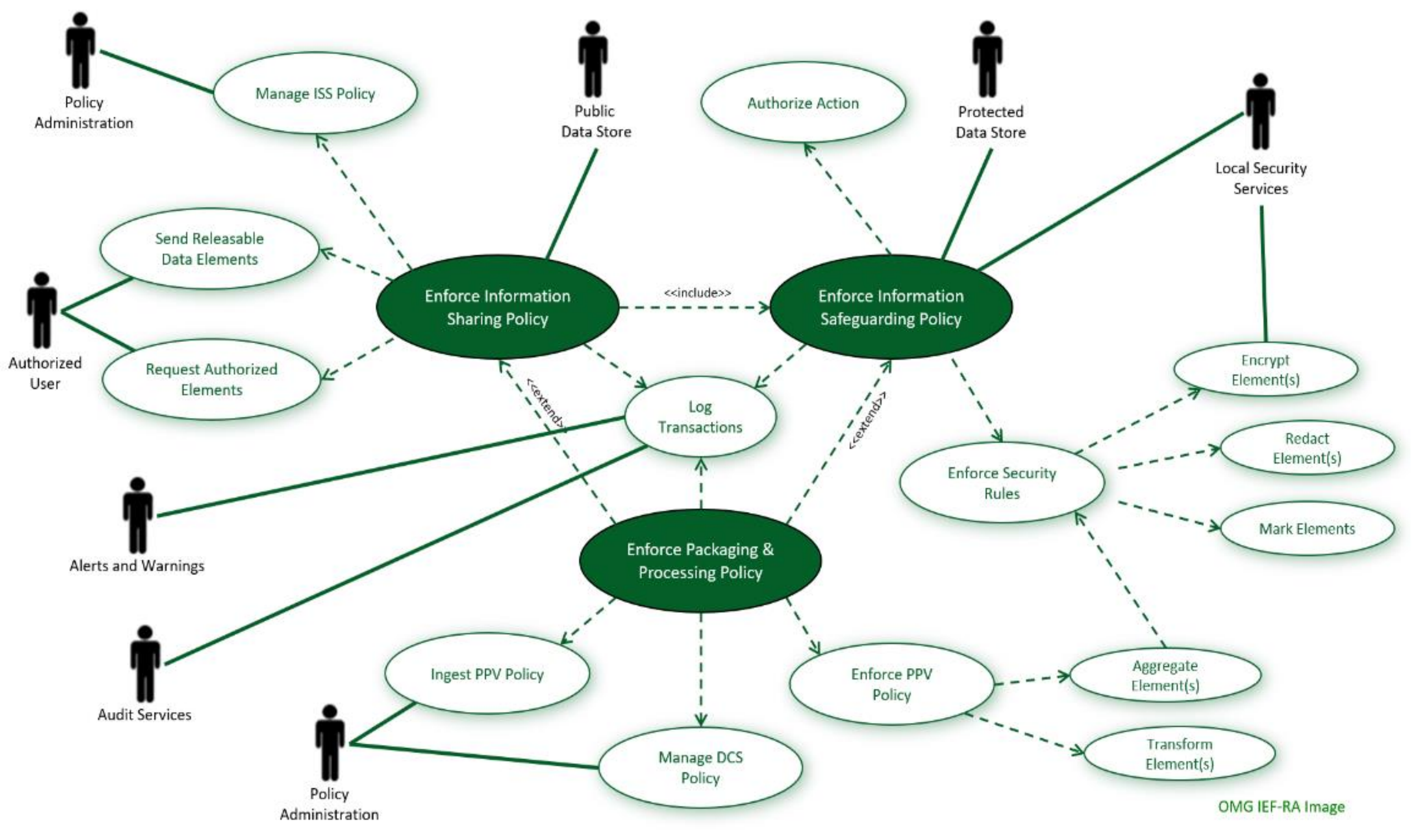
Why Focus on Data Centric Security

- Data Centric Security (DCS):
  - Focusses on applying security at the data and information layer
  - Applicable to Secure Email, Chat, File-Share, system-to-system (S2S) exchanges
  - Enables Information Sharing and Safeguarding (ISS) tailored to recipient need and authorizations
  - Enables system-to-system ISS within and across organizations, domains, national and international Partners
- ISS is the foundation for:
  - Delivering Information and Decision Advantage
  - Delivering All Domain C4I, operations, incident management and program delivery
  - Delivering Cyber Security (e.g., Cyber SA and Intelligence)
  - Collapsing of the CAF Networks
  - Enabling the DND/CAF to interoperate
  - And more
- Sharing and Safeguarding are integrated mutually reinforcing Concepts
  - DCS Aligns and Integrates Information Sharing and Information Safeguarding
  - The DND/CAF Demonstrating the Ability to Effectively Safeguard Sensitive Information – Will Increase Partner Trust – and Increase their Willingness to Share their Information
  - Separate Sharing and Safeguarding and Initiatives to Deliver Interoperability Will Fail (decades of failed effort prove this point)
- Another layer in and Defence-in-Depth Approach

Element of ISS

To be effective sharing and safeguarding cannot be separated

Going Forward, the CAF to Evolve ISS and DCS Competencies



OMG IEF-RA Image

Focus of Canadian International Efforts to Deliver Interoperability

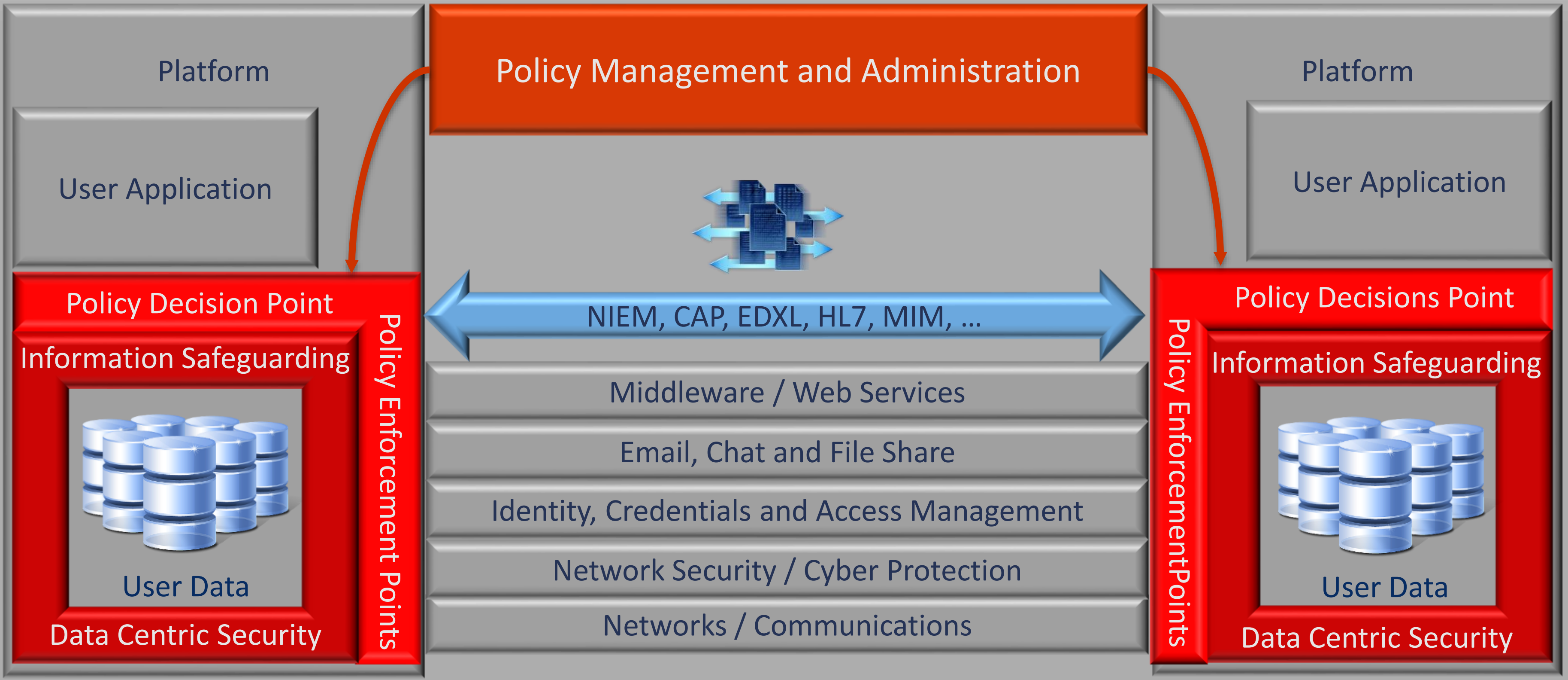
Canadian Focus is on:

1. Information Sharing and Safeguarding
2. Data Centric Security
3. ISS Policy Administration

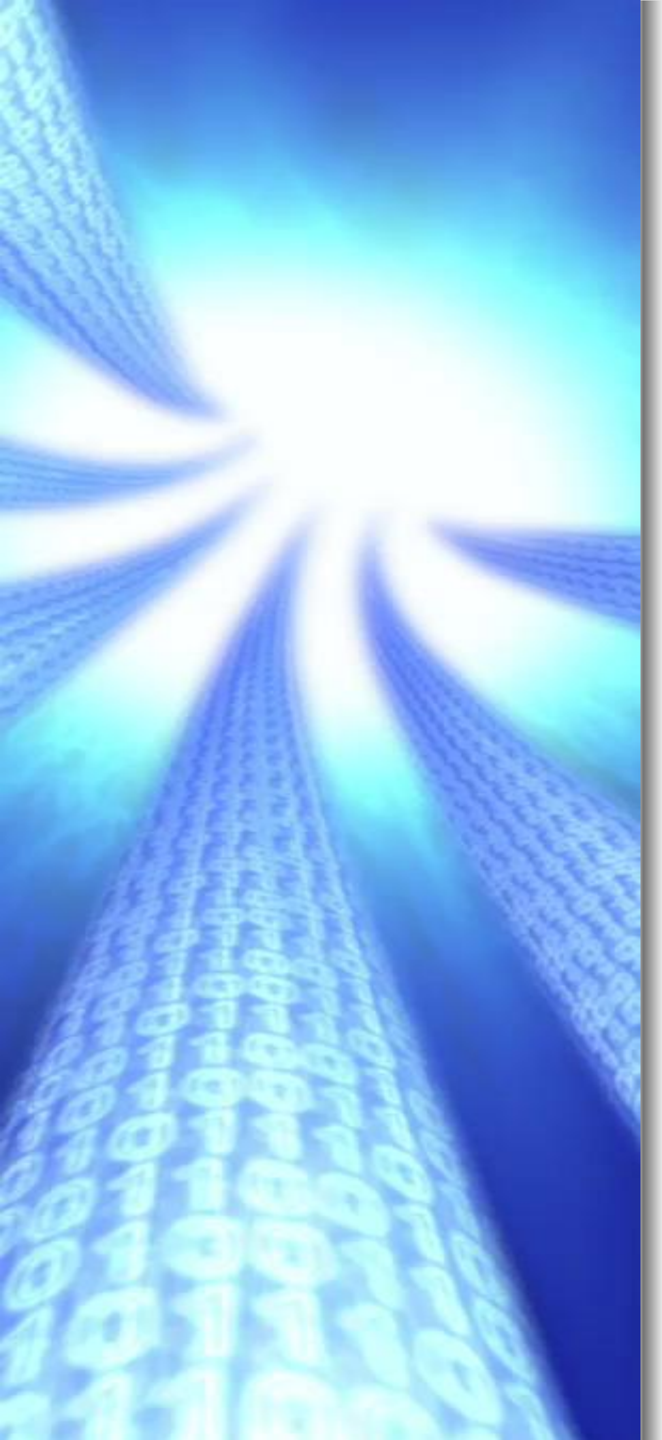
Efforts include:

1. DCS Lead at CWIX and TIDE Sprint
2. OMG Information Exchange Framework

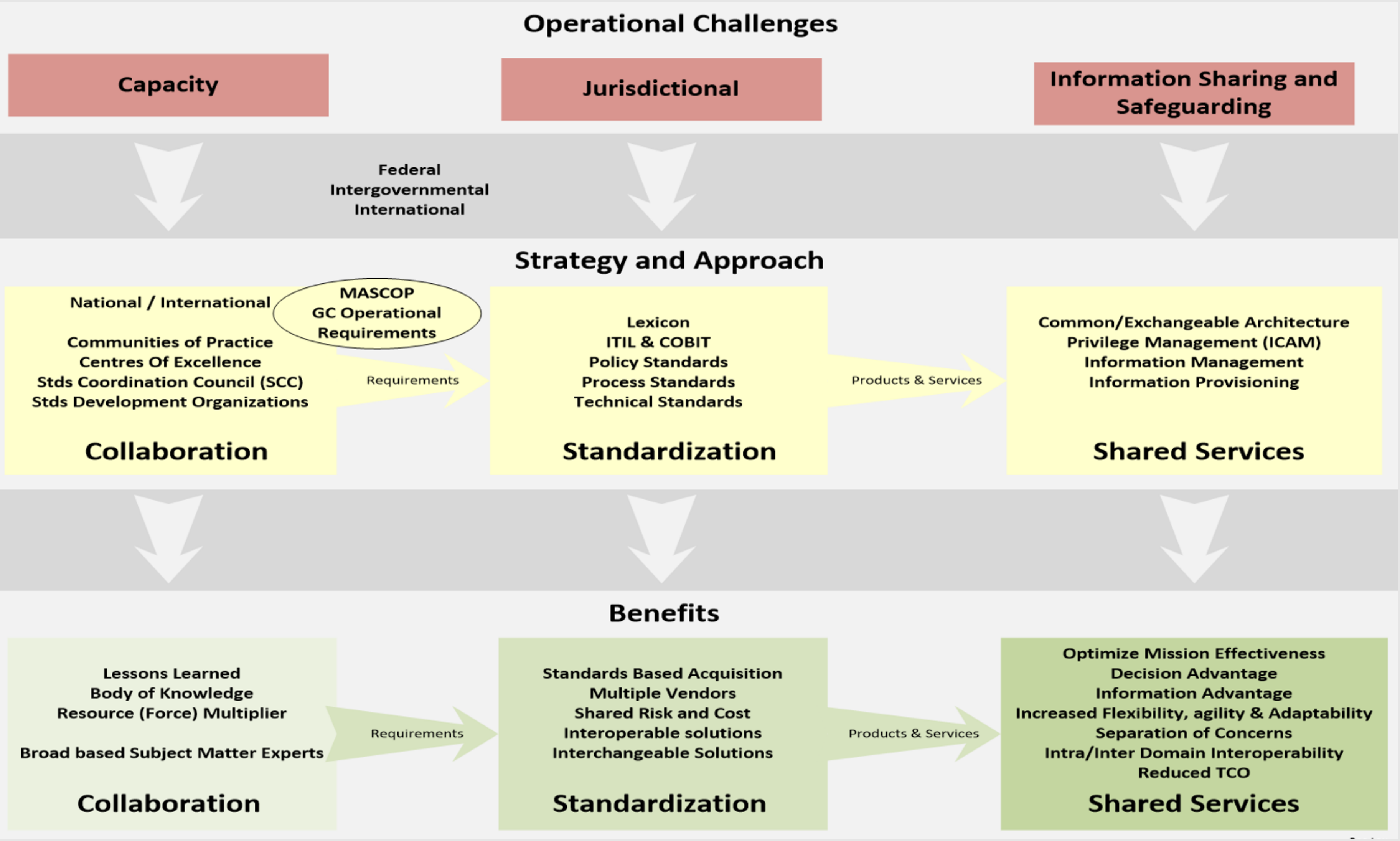
Seeks to leverage other international standards and initiatives (e.g., NIEM)



Platform
User Application
Policy Decision Point
Information Safeguarding
User Data
Data Centric Security
Policy Enforcement Points
Policy Management and Administration
NIEM, CAP, EDXL, HL7, MIM, …
Middleware / Web Services
Email, Chat and File Share
Identity, Credentials and Access Management
Network Security / Cyber Protection
Networks / Communications
Platform
User Application
Policy Decisions Point
Information Safeguarding
User Data
Data Centric Security
Policy EnforcementPoints



Vision and Value Proposition



Operational Challenges

Capacity

Jurisdictional

Information Sharing and Safeguarding

Federal
Intergovernmental
International

Strategy and Approach

National / International

MASCOP
GC Operational
Requirements

Communities of Practice
Centres Of Excellence
Stds Coordination Council (SCC)
Stds Development Organizations

Collaboration

Requirements

Lexicon
ITIL & COBIT
Policy Standards
Process Standards
Technical Standards

Standardization

Products & Services

Common/Exchangeable Architecture
Privilege Management (ICAM)
Information Management
Information Provisioning

Shared Services

Benefits

Lessons Learned
Body of Knowledge
Resource (Force) Multiplier

Broad based Subject Matter Experts

Collaboration

Requirements

Standards Based Acquisition
Multiple Vendors
Shared Risk and Cost
Interoperable solutions
Interchangeable Solutions

Standardization

Products & Services

Optimize Mission Effectiveness
Decision Advantage
Information Advantage
Increased Flexibility, agility & Adaptability
Separation of Concerns
Intra/Inter Domain Interoperability
Reduced TCO

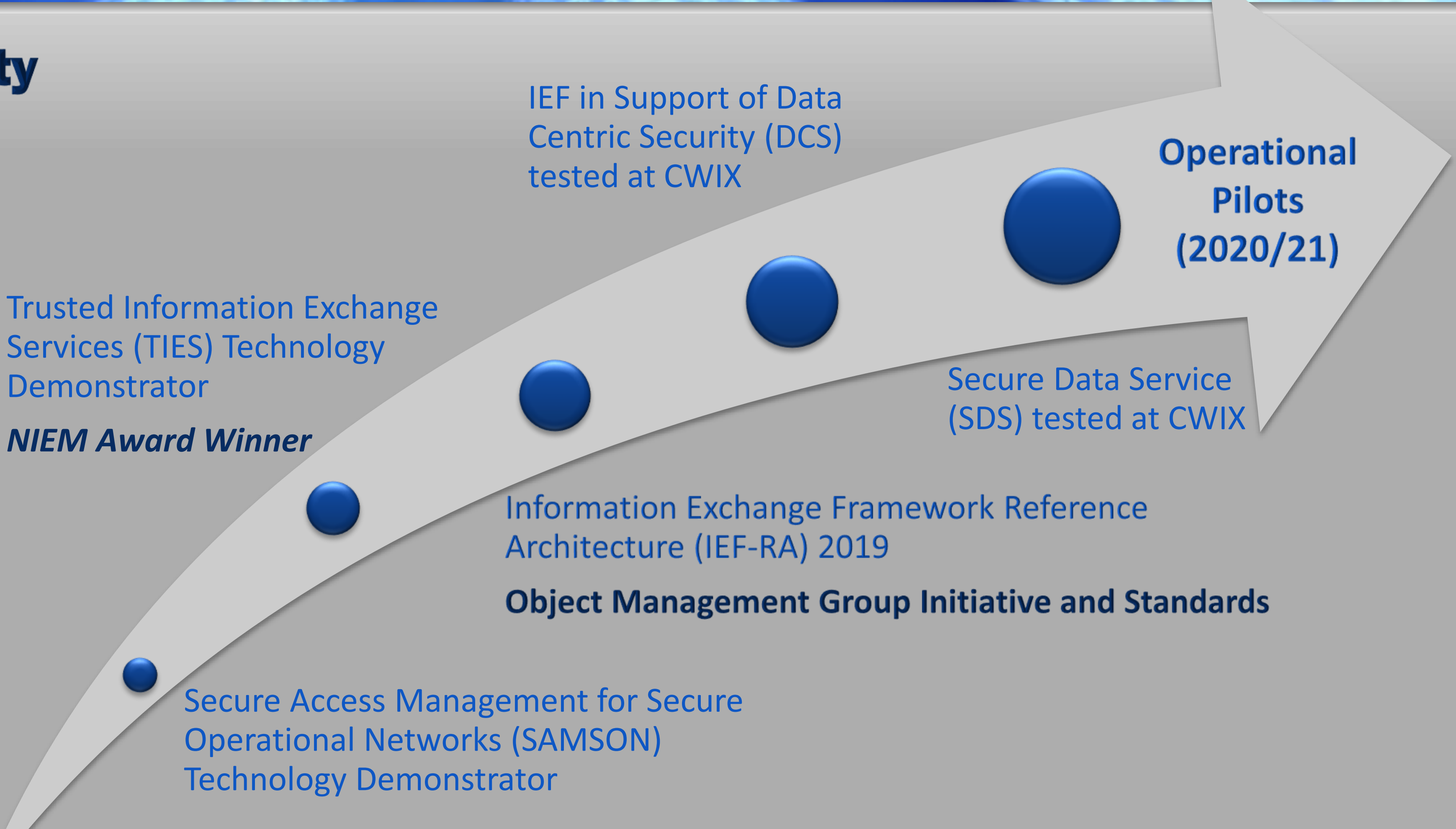
Shared Services

Evolution of ISS Capability

Canadian innovation is based a progression of:

1. Understanding
2. Standardization
3. Abstraction
4. Automation

Understanding is based on the evaluation, experimentation, testing and demonstration of technology demonstrators



Secure Access Management for Secure Operational Networks (SAMSON) Technology Demonstrator

Trusted Information Exchange Services (TIES) Technology Demonstrator

NIEM Award Winner

Information Exchange Framework Reference Architecture (IEF-RA) 2019

Object Management Group Initiative and Standards

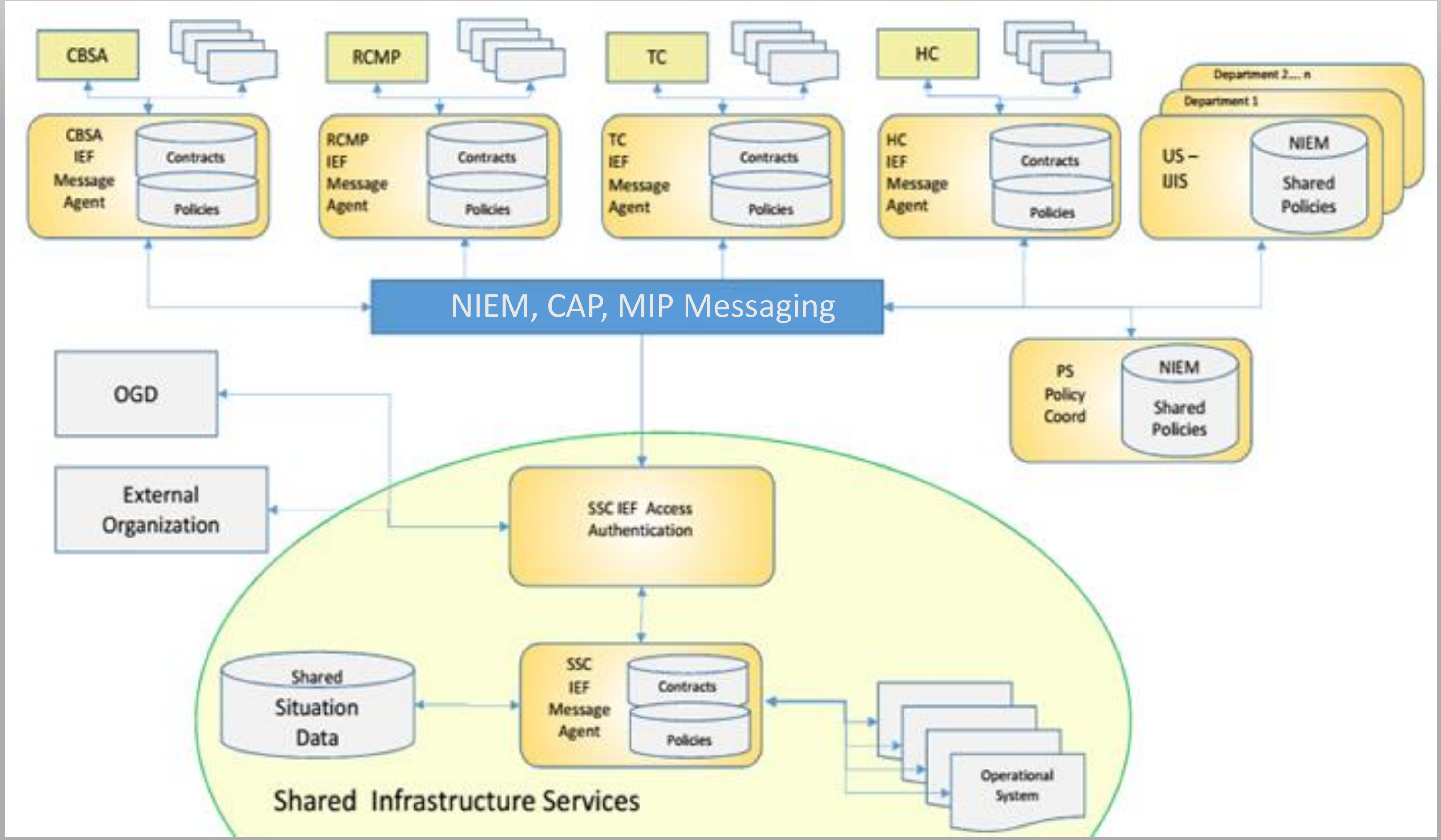
IEF in Support of Data Centric Security (DCS) tested at CWIX

Secure Data Service (SDS) tested at CWIX

Operational Pilots (2020/21)

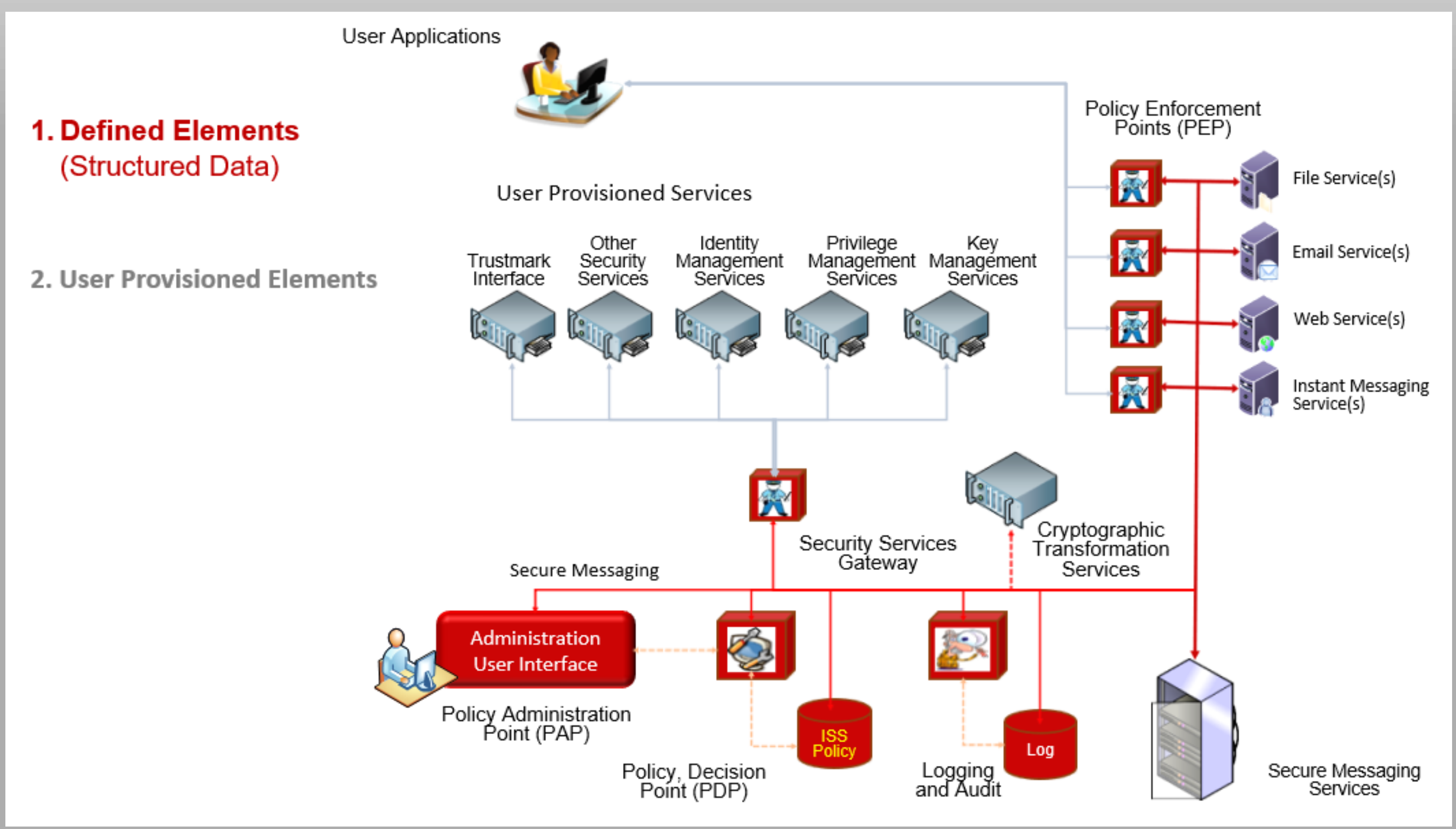
Trusted Information Exchange Services Technology Demonstration

- Demonstrate selective sharing of incident data between partners based on policies
- Multiple Government of Canada Stakeholders
- Information the development of the OMG IEF Initiative
- Best of NIEM Award



Secure Access Management for Secure Operating Networks

- Enable the Canadian Forces to securely operate on coalition operational networks
- Focussed on Email, File-Share, and Chat
- Design documents contributed to the OMG IEF Initiative forming the foundation of the IEF Reference Architecture
- Foundation of the NATO and TIDE Sprint DCS functional areas led by Canada



1. Defined Elements (Structured Data)

2. User Provisioned Elements

User Applications

User Provisioned Services

Trustmark Interface

Other Security Services

Identity Management Services

Privilege Management Services

Key Management Services

Policy Enforcement Points (PEP)

File Service(s)

Email Service(s)

Web Service(s)

Instant Messaging Service(s)

Security Services Gateway

Cryptographic Transformation Services

Secure Messaging

Administration User Interface

Policy Administration Point (PAP)

ISS Policy

Policy, Decision Point (PDP)

Log

Logging and Audit

Secure Messaging Services

Focus of Canadian International Efforts to Deliver Interoperability (CWIX 2018/19/20)

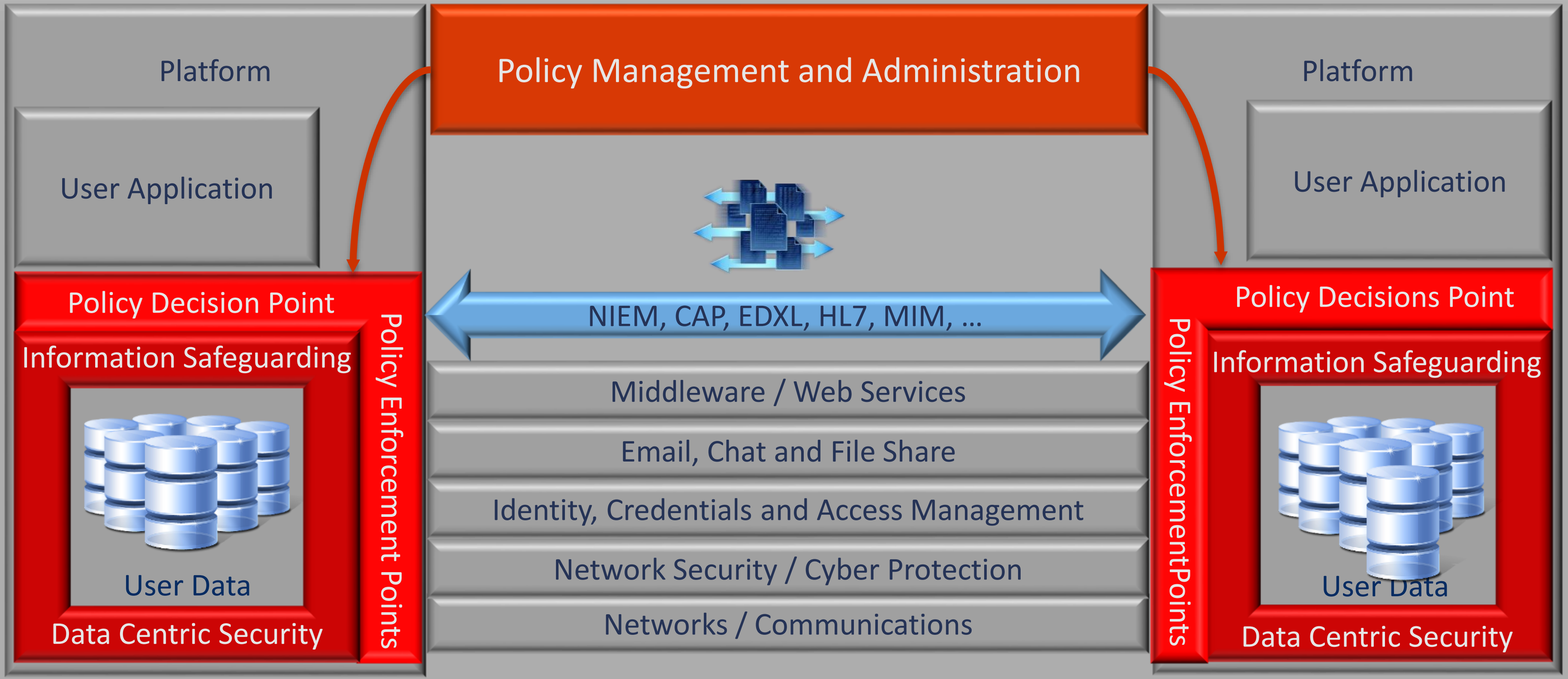
Canadian Focus is on:

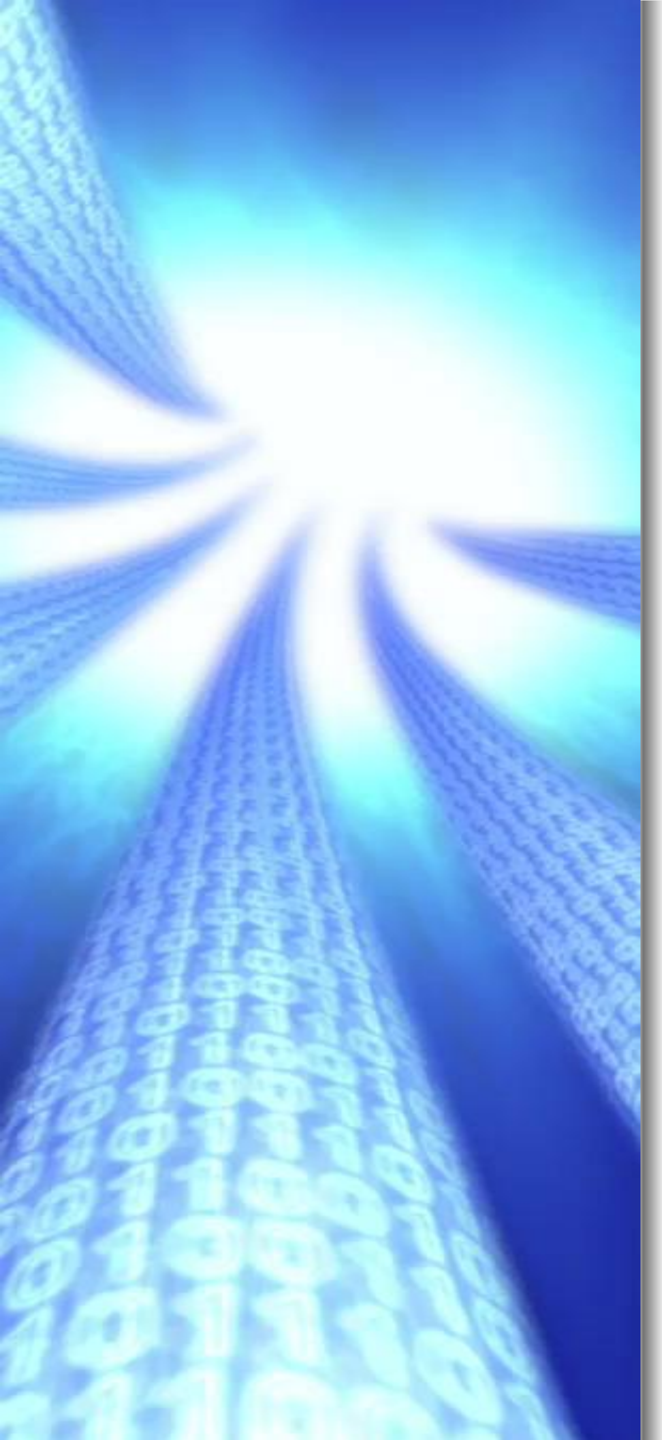
1. Information Sharing and Safeguarding
2. Data Centric Security
3. ISS Policy Administration

Efforts include:

1. DCS Lead at CWIX and TIDE Sprint
2. OMG Information Exchange Framework

Seeks to leverage other international standards and initiatives (e.g., NIEM)


Platform
User Application
Policy Decision Point
Information Safeguarding
User Data
Data Centric Security
Policy Enforcement Points
Policy Management and Administration
NIEM, CAP, EDXL, HL7, MIM, …
Middleware / Web Services
Email, Chat and File Share
Identity, Credentials and Access Management
Network Security / Cyber Protection
Networks / Communications
Platform
User Application
Policy Decisions Point
Information Safeguarding
User Data
Data Centric Security
Policy EnforcementPoints



Current ISS / DCS Objectives

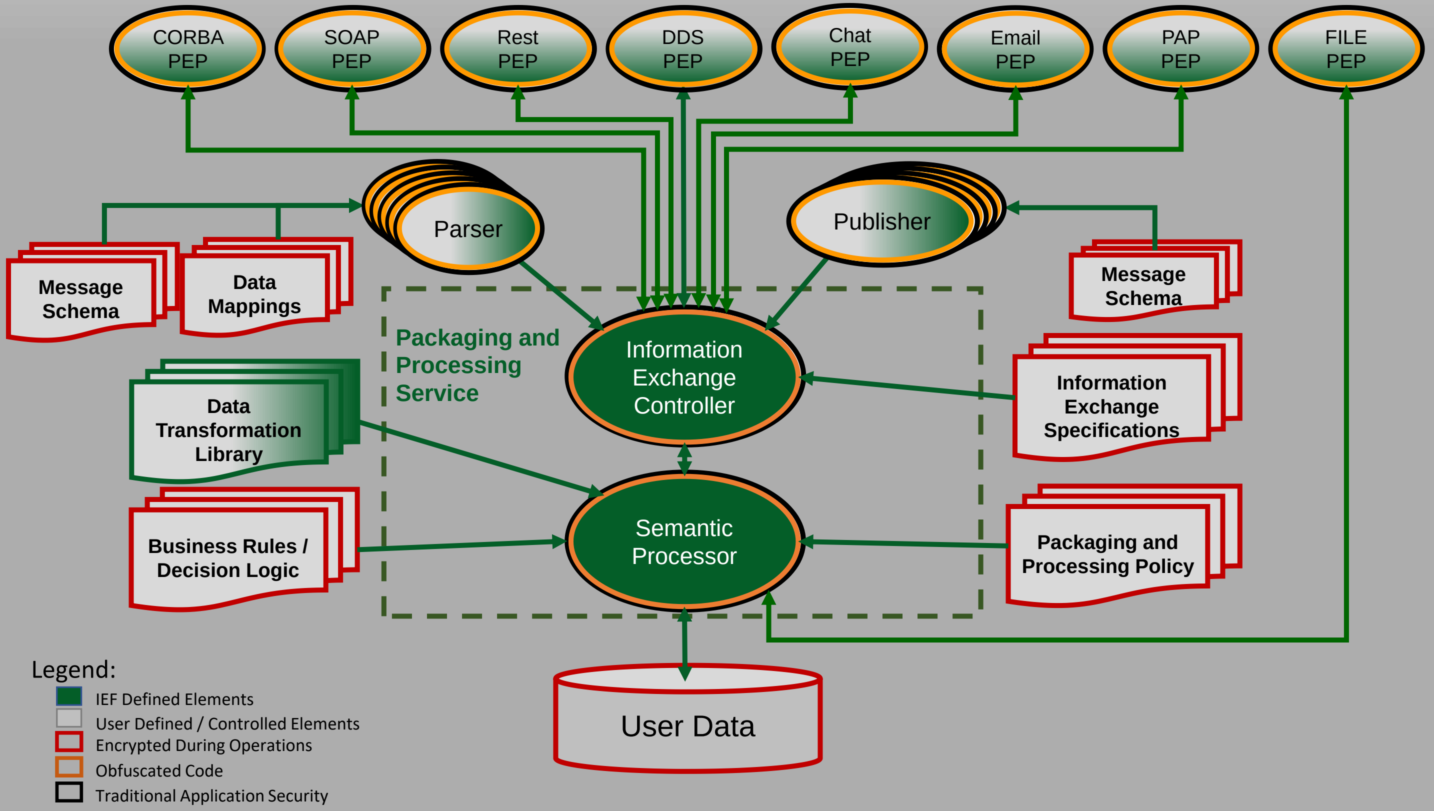
- Data Centric Security
  - Automated ISS Policy Enforcement:
    - Selective Sharing of Data based on need and authorization
    - Automated labeling of messages
  - Secure Deployable Data Service
  - Secure Data as a Service
  - Secure Data Pool
  - Integration of policy administration during operations

- ISS
  - Cross Domain Information Sharing
  - Automated Labeling of messages

- Information Advantage
  - Secure and selective routing of data and information through mission threads (e.g., targeting, Intelligence, Situational Awareness, and/or decision aids)
  - Application of DCS in an analytics pipeline

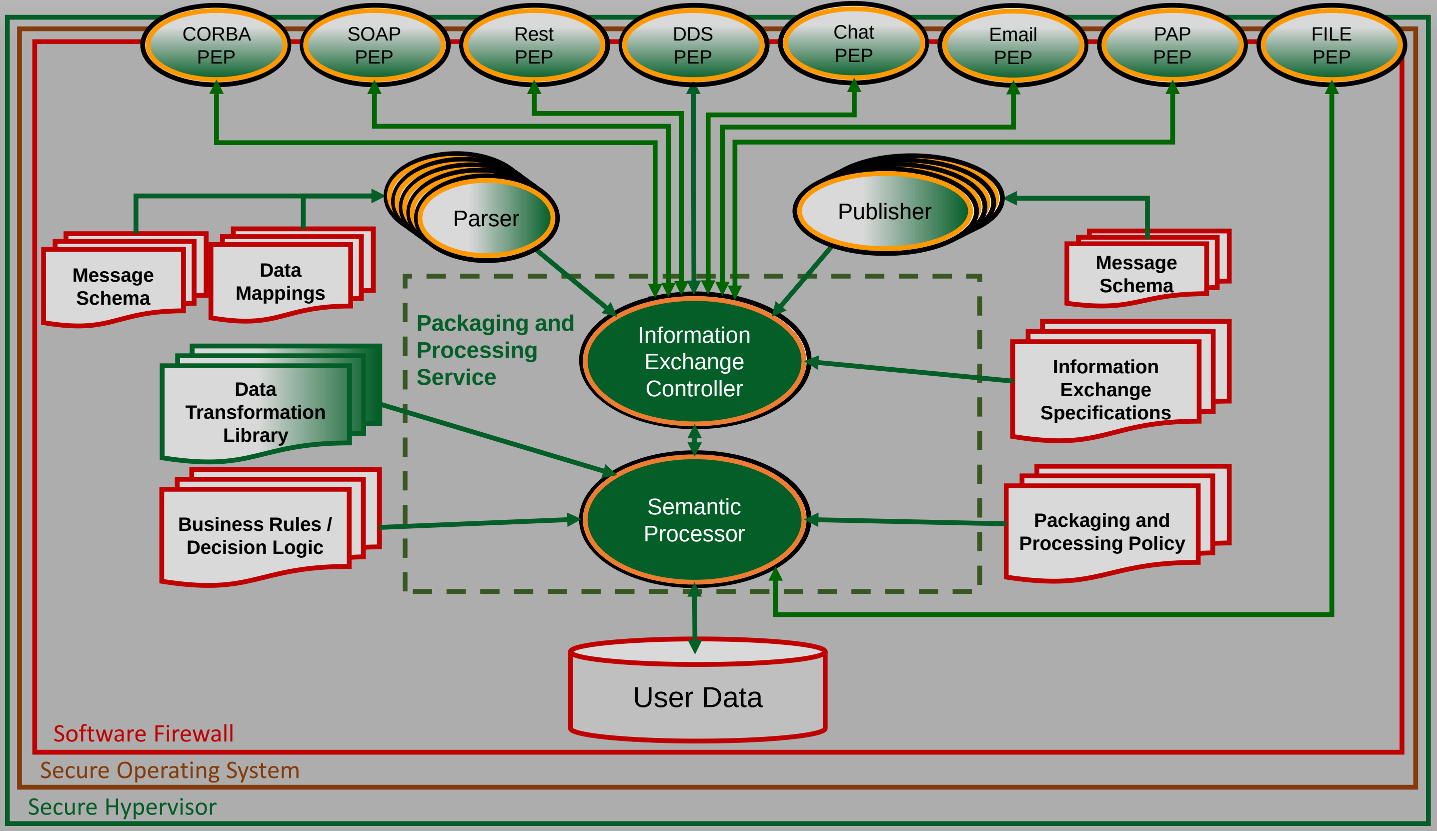
Secure Packaging and Processing of Data (tested in TIES and CWIX 2018/19/20)

- DCS PEP = Semantic Processor + Information Exchange Controller + PEP
  - Semantic Processor assures that only authorized content is released to each recipient
  - Information Exchange verifies releaseability based on aggregated content, formats the message and routes the message to the specified infrastructure - services the users information sharing agreements
  - The PEPs provide the Integration Point to the users own infrastructure, and access and release control using User Security services (e.g., ICAM)
- Policies, configurations, transforms are separated from the service code to:
  - Increase ownership for the user
  - Increase flexibility, Agility and adaptability
  - Enable runtime administration of ISS operations


CORBA PEP
SOAP PEP
Rest PEP
DDS PEP
Chat PEP
Email PEP
PAP PEP
FILE PEP
Parser
Publisher
Message Schema
Data Mappings
Message Schema
Packaging and Processing Service
Information Exchange Controller
Information Exchange Specifications
Data Transformation Library
Semantic Processor
Business Rules / Decision Logic
Packaging and Processing Policy
User Data
Legend:
🟩 IEF Defined Elements
□ User Defined / Controlled Elements
🟥 Encrypted During Operations
🟧 Obfuscated Code
□ Traditional Application Security

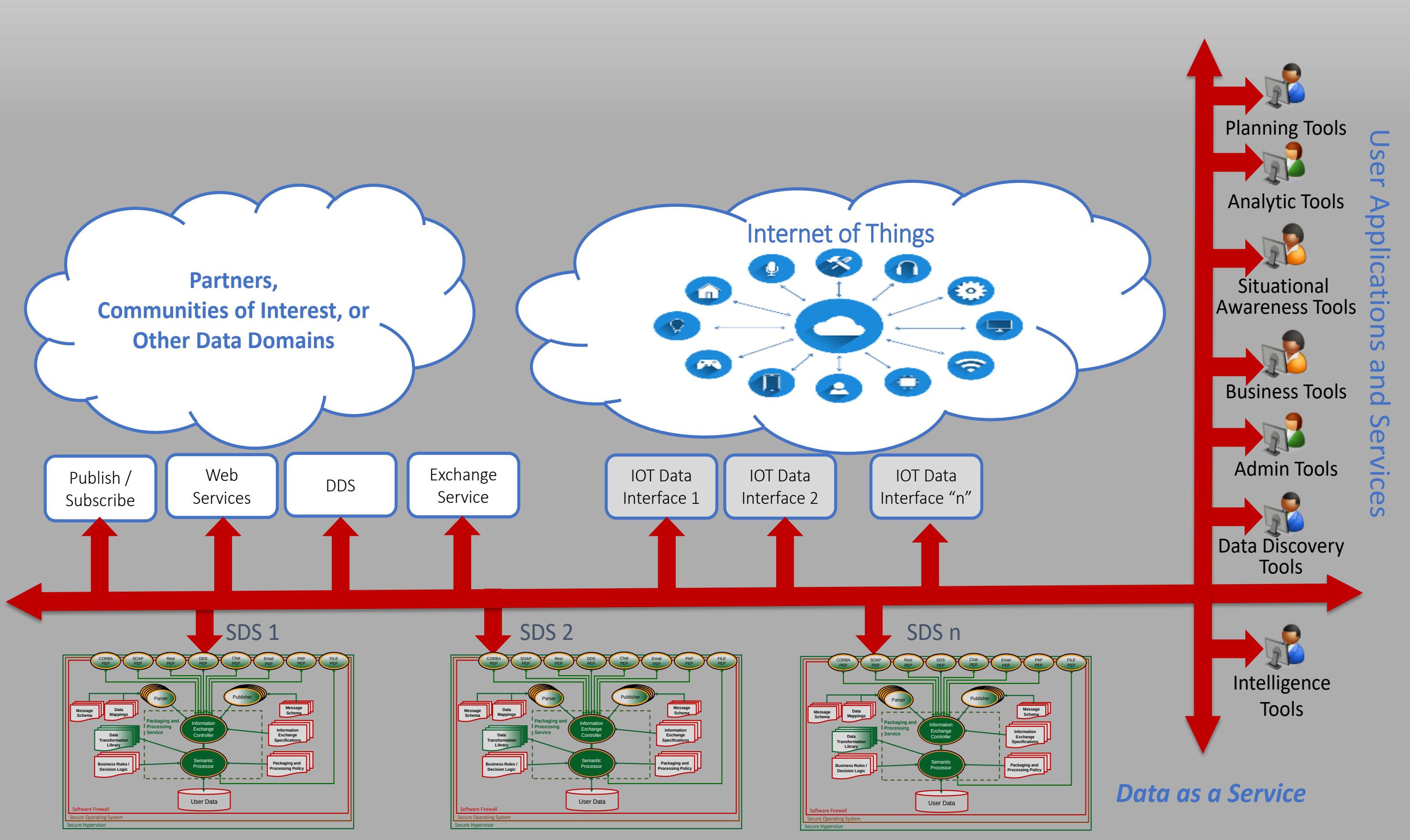
Secure Data Service (Tested CWIX 2020)

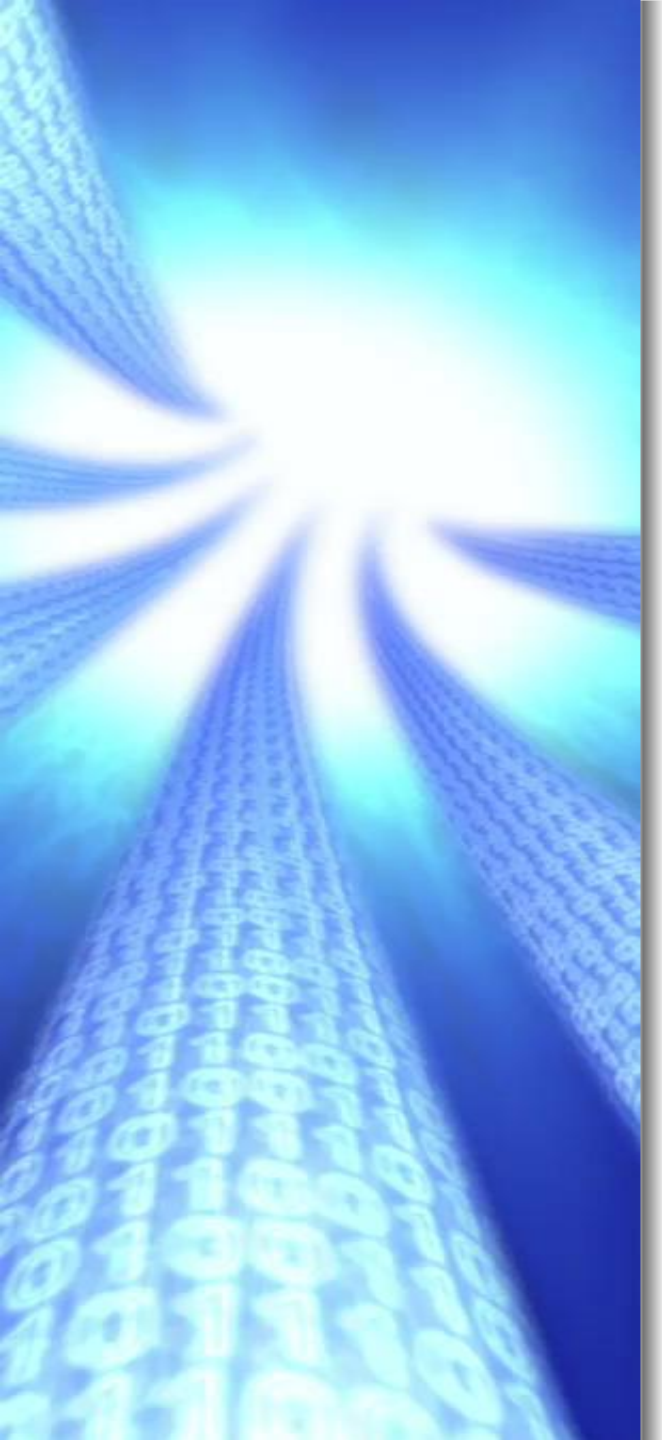
- Provide Data as a Service (DaaS)
- Minimize the vectors of attack on the DaaS (Packaging and Processing Services and User Data)
    - VM configured to PEP access Only
    - OS Policy limits operation to SDS services Only
    - Firewall Policy limits access to PEP Ports Only
    - Code is obfuscated to inhibit tampering
    - User data encrypted at rest & in transit
    - Policies, configurations and transformation encrypted to inhibit tampering
- Controls the content released based on recipient(s) need and authorization



Employing a SDS (CWIX 2021)

- **DCS enabled DaaS as a Service Implementation that provides for:**
  - Automated ISS policy enforcement
  - The secure deployment of data
  - The provision of common and sharable data for multiple independent interface and user applications
  - The flexible, agile, and adaptive configuration and deployment of ISS Capability
- Scheduled for testing at CWIX 2021
- Multiple in-years tests and demonstrations planned

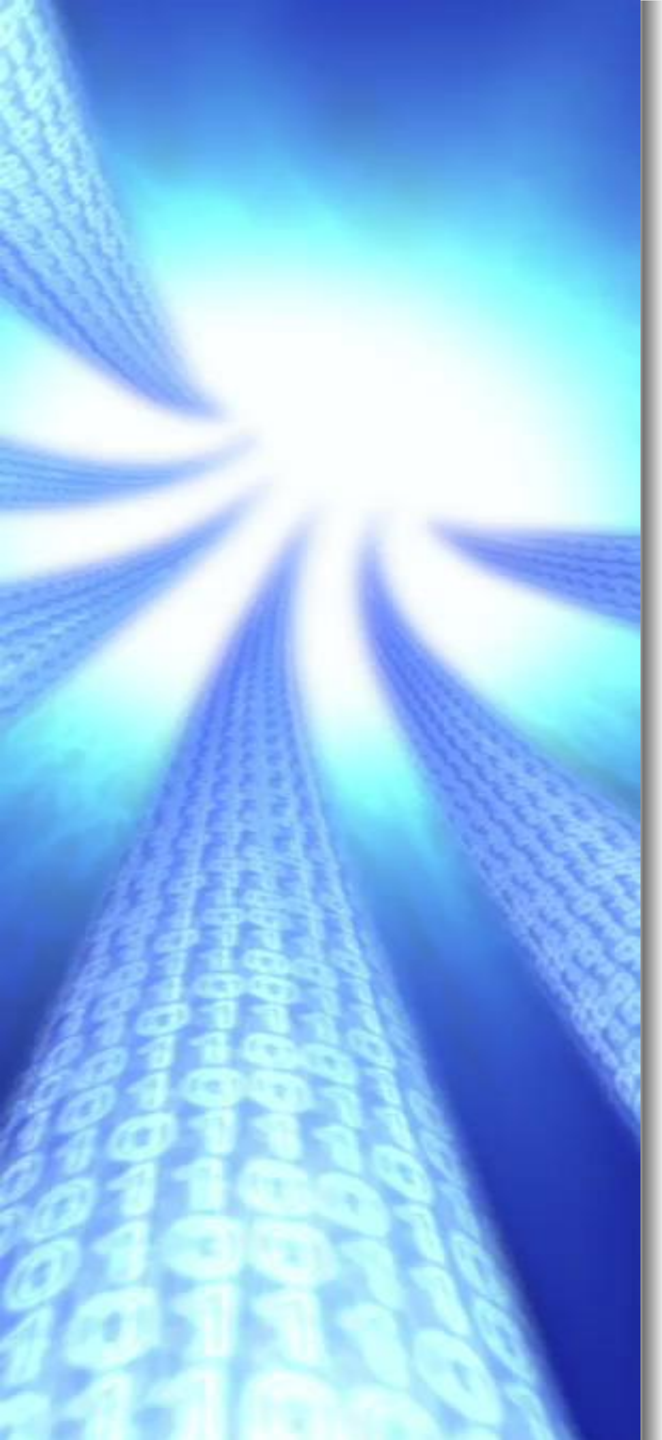




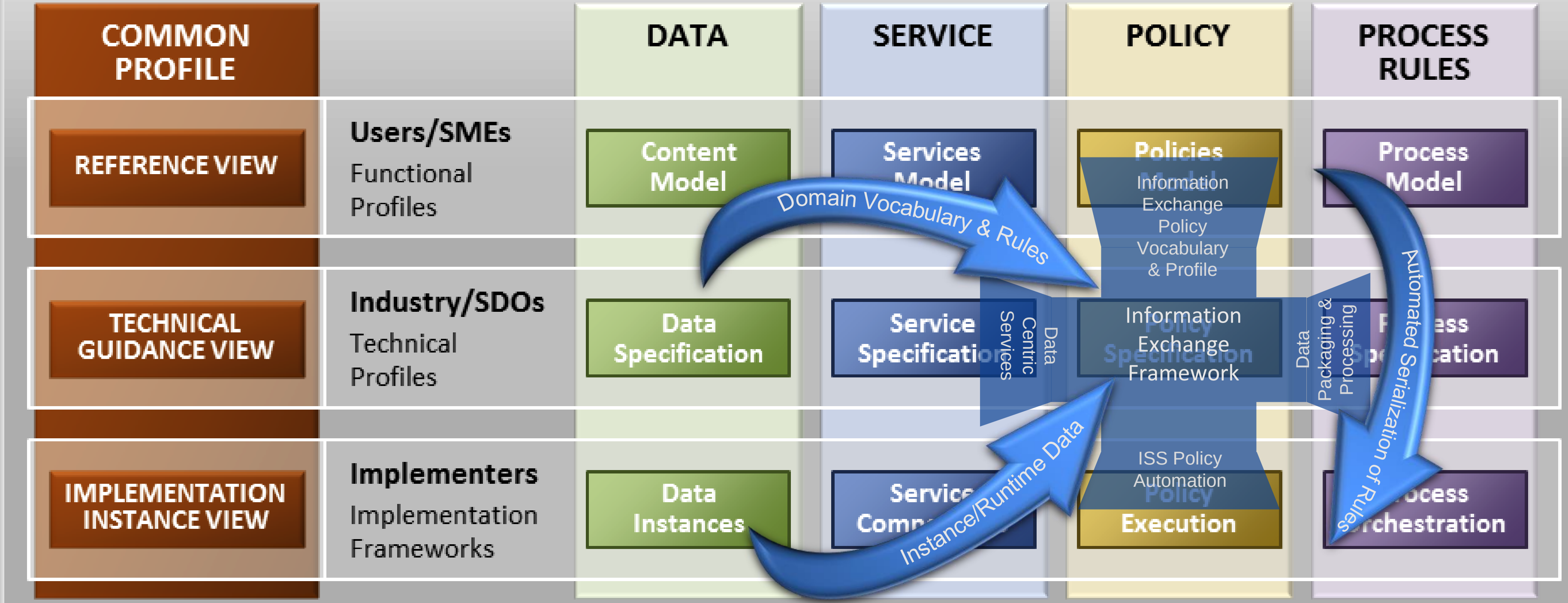
Take-away

- Common Semantics (e.g., NIEM) ne in a number of tool needed to deliver Information Sharing and Safeguarding (ISS)
- Cannot separate the sharing from the safeguarding of data and deliver broad-based ISS
- Data Centric Security (DCS) will enable used to balance the mandate to share with the responsibility protect

Questions? More Information?



IEF Overlay for PM-ISE Interoperability Framework



COMMON PROFILE		DATA	SERVICE	POLICY	PROCESS RULES
REFERENCE VIEW	**Users/SMEs** Functional Profiles	Content Model	Services Model	Policies Model	Process Model
TECHNICAL GUIDANCE VIEW	**Industry/SDOs** Technical Profiles	Data Specification	Service Specification	Policy Specification	Process Specification
IMPLEMENTATION INSTANCE VIEW	**Implementers** Implementation Frameworks	Data Instances	Service Components	Policy Execution	Process Orchestration

Domain Vocabulary & Rules

Information Exchange Policy Vocabulary & Profile

Data Centric Services

Information Exchange Framework

Data Packaging & Processing

ISS Policy Automation

Instance/Runtime Data

Automated Serialization of Rules