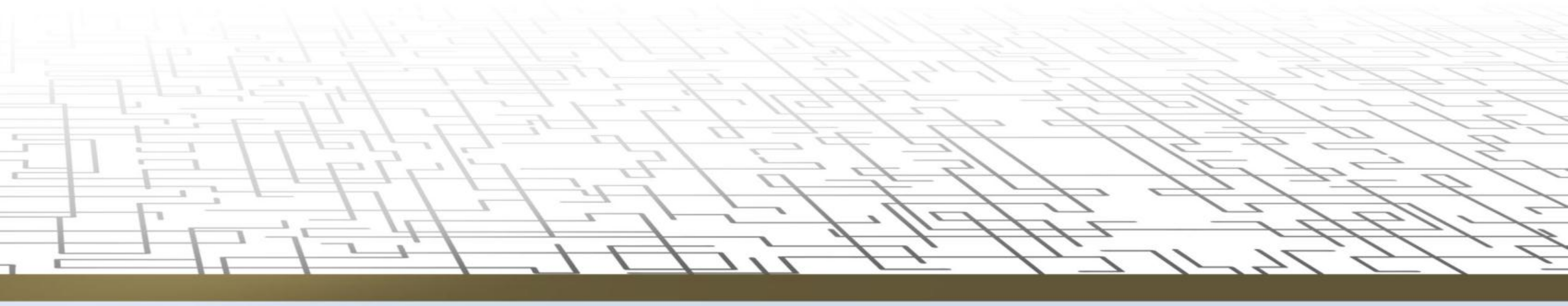


Information Sharing Environment

Information Integration Subcommittee

Information Sharing Exercise

Participant Package

Version 2.1

Name:

Agency:

Contact Info:

System/Capability:

Table of Contents

Introduction

"It is a national priority to efficiently, effectively, and appropriately share and safeguard information so any authorized individual (Federal, state, local, tribal, territorial, private sector or foreign partner) can prevent harm to the American people and protect national security. The Strategy points toward a future in which information support national security decision-making by providing the right information, at any time, to any authorized user, restricted only by law or policy, not technology; and where safeguarding measures, to include a comprehensive regimen of accountability, prevent the misuse of the information."

This passage from the National Strategy for Information Sharing and Safeguarding (NSISS) establishes the National vision for information sharing. The NSISS goes on to identify three information sharing principles:

1. Information as a National Asset
2. Information Sharing and Safeguarding Requires Shared Risk Management
3. Information Informs Decision Making

Supporting these principles are 16 priority objectives. Focusing on Priority Objective 6, "Define and adopt baseline capabilities and common requirements to enable data, service, and network interoperability", and supporting the second principle, the office of the Program Manager - Information Sharing Environment (PM-ISE) has developed the "Information Sharing Environment Interoperability Framework (I^{2}F)". The I^{2}F works to guide alignment of the various Federal, Department or Community architectures through the definition of common architectural domains; Business, Data, Applications & Systems, Infrastructure, Security, and Performance.

To assist program managers in assessing system interoperability, the I^{2}F utilizes an interoperability maturity matrix. The I^{2}F maturity matrix defines the various functions and processes, along with common levels of performance, for each architectural domain, less Infrastructure. This exercise utilizes a subset of the I^{2}F maturity model that is based on MDA-specific mission needs and architectural principles.

To ensure the applicability of the I^{2}F maturity model, the Information Integration Sub-Committee (IISC) will be executing an information sharing exercise. The intent of the exercise is to evaluate the maturity model and guide development of the I^{2}F.

The exercise will utilize the information sharing process defined in the National Maritime Domain Awareness (MDA) Architecture Plan as a *reference* architecture. As such, the exercise will also evaluate an initial set of security attributes to manage the shared information and determine the operational relevance of the exchange models used by the maritime community.

This assessment will provide the information required to execute the exercise.

Scenario General Description

It's 9:45 am on July 4th. Terrorists from the Universal Grievance Group (UGG) access a fixed HAZMAT facility on the Detroit River via two 16 foot aluminum boats. They quickly launch rocket-propelled grenades (RPGs), resulting in major fires. The two boats depart, one heading north, one heading south. At the same time, a Canadian river boat explodes nearby with 200 passengers onboard.

The wind is headed towards Windsor, Ontario, and there is a large, heavy plume of smoke. Releases of cobalt, nickel, molybdenum, cadmium, mercury, vanadium, platinum, and other metals have occurred in the plume. Casualties occur at the HAZMAT facility due to the explosive blast and fragmentation, fire, and vapor/liquid exposure to the toxic industrial chemical (TIC). Casualties also occur on the Canadian river boat with victims observed in the surrounding water.

This scenario is not designed to evaluate response. This scenario is to facilitate the identification of information exchange requirements and interoperability gaps. All participants are expected to have coordinated with their internal stakeholders to exercise their internal processes prior to the execution of the exercise. The exercise will focus on information exchange and interoperability requirements resulting from planned response processes.

Timeline/Events

As these events unfold, focus on what information you would receive from an external organization and what information you would distribute to an external organization. - Who would notify you, and who would you notify?

0945 – Two small 16 foot aluminum motor vessels (MVs) inbound to a clearly marked restricted area surrounding the HAZMAT facility

Inject 1: Is there concern? Who would monitor the area? Would you have means to ID the boats?

1000 – MVs launch RPGs on HAZMAT facility which then explodes

Inject 1: Public Transportation Closures (i.e., all tunnel traffic, airport, bus stations, etc.)

Inject 2: There are casualties

1000 – Canadian river boat explodes with 200 passengers onboard

Inject 1: Boat Status? –Sinking boat with oil in the water

Inject 2: Passengers' status? – Casualties with 5 in water

Inject 3: Passengers' Citizenship? – 3 French, 194 Canadian passengers, and 3 Americans

1010 – One small boat heads north, one heads south

Inject 1: Do you notify different D/As of where the boats are going?

1025 – First responders ID HAZMAT facility as toxic scene

Inject 1: Who would you, as the first responder, notify as a result of the toxic material being in the facility? – Or if you are not a first responder, how would you be notified?

Inject 2: Critical infrastructure impact (i.e., water treatment facilities)

1030 – Toxic plume moves towards Windsor

Inject 1: U.S. Public Notification – Possible Evacuation

Inject 2: Canadian Authority Notification

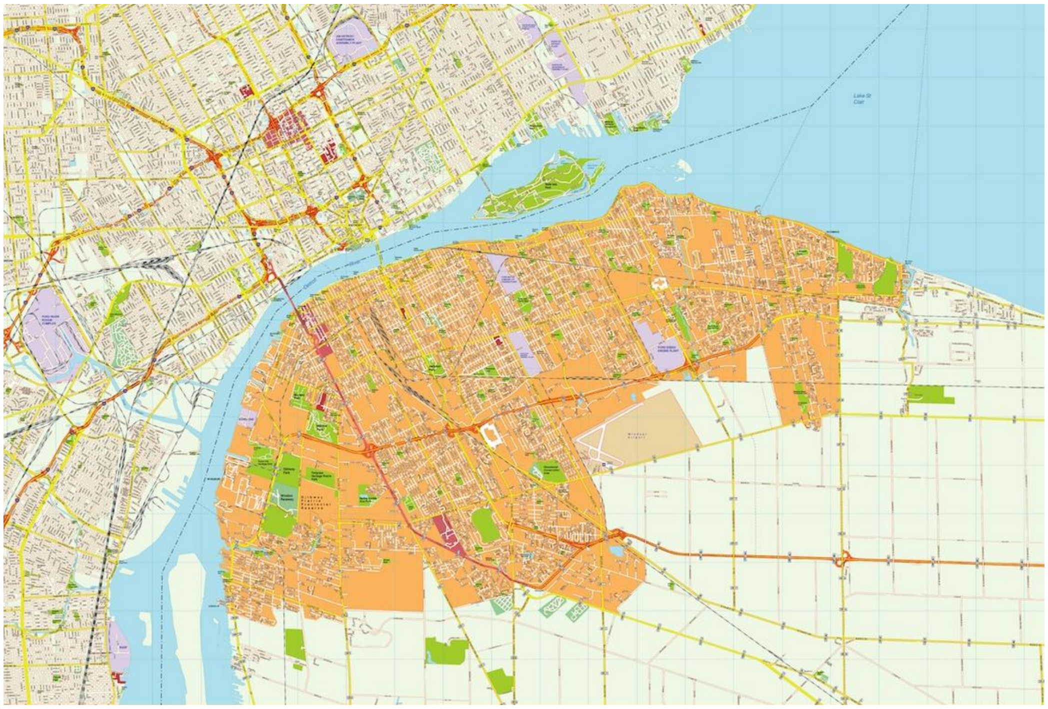
1045 – Oil in water around Canadian river boat

Inject 1: Environmental hazards

Detroit Maps

Royal Oak
Lake St. Clair
hfield
Eastpointe
Harper Woods
Highland Park
Grosse Pointe
DETROIT
y
Windsor
earborn
South Walkerville
Park
Fairplay
troit River
Essex
ew

Map A – River Overview



Map B– Metro Area Overview

Business Domain Interoperability Objectives

The business domain ensures the system or program architecture (*reference architecture*) aligns to an organization's mission requirements and clearly describes the scope, goals, and purpose of the architecture. The business domain describes:

- References to policies, guidance, and laws that affect the reference architecture and related mission objectives
- Governance groups responsible for oversight of the reference architecture
- Mission vision, objectives, and requirements
- Lines of business, capabilities, and activities
- Planned achievement of capabilities by timeframes and what constrains/policies apply

Interoperability Objectives

Interoperability objectives for the business domain include:

- Description of how a reference architecture supports the operational enterprise
- Incorporating information sharing functions into mission-specific activities (e.g., address the information sharing lifecycle activities such as collection, analysis, dissemination, storage, and retirement)
- Using standards-based approaches to capture business requirements and document business processes and information flows
- Identifying common information exchanges for a specific mission scenario/use case
- Capturing information sharing requirements, constraints, and rules between partners

Assessment

The Business Domain is divided into function or process groups. The following pages provide an overall assessment of each group including several supporting questions. Using the matrix below, please complete the assessment.

	①: Ad-hoc	②: Repeatable	③: Enhanced	④: Managed	⑤: Optimized
Business Process Definition	Formalized definitions of the business processes do not exist	Definitions of the business processes are formalized and understood within the organization	The formalized definitions of the business processes are understood by external partners	Internal and external partners understand the various roles within the business process through manual workflows	All internal and external partners understand the various roles within the business process through automated workflows
Business Process Models	Formalized business process models that describe the information sharing flows are not defined	Business process models that describe the information sharing flows are defined by a modeling standard and are aligned to applicable policy, guidance, or law. The models employ repeatable exchange patterns	The formalized business process models are understood by external partners, interoperable, and can be manually provided to authorized users	The formalized business process models are available online to authorized users	The formalized business process models use a modeling standard (e.g. BPMN, WS-BPEL, IDEF0, or XPDL 2.1) and share and reuse processes.
Information Sharing Agreements (ISAs)	An ISA does not exist	The ISA documents the purpose, scope, and authorized users of the data exchanges	The ISA is understood by all users who are involved in the data exchanges and can be manually provided to authorized users	The ISA is available online to authorized users and compliance is manually monitored	Compliance to the ISA is automated. Metrics are collected and used to enhance interoperability across agencies

Business Domain Review

1.0	**Overall Business Process Definition**	①②③④⑤
1.1	Does your agency utilize a common (reference) architectural model to develop enterprise capabilities?	👍Yes 👎No
1.2	Does your agency map exchange processes to include exchange triggers, controls or rules, outputs, technologies, or standards used to perform the exchange?	👍Yes 👎No
1.3	Does your agency document the information exchanges required to accomplish its mission?	👍Yes 👎No
2.0	**Overall Business Process Model**	①②③④⑤
2.1	Does your agency incorporate information sharing functions into its mission-specific activities?	👍Yes 👎No
2.1.1	Are those functions defined as an integrated part of the mission activities?	👍Yes 👎No
2.2	Does your agency use a standards-based approach to capture business requirements, document business processes, and information flows (e.g.: BPMN, IDFE0, UML)?	👍Yes 👎No
3.0	**Information Sharing Agreements (ISAs)**	①②③④⑤
3.1	Does your agency have standard polices that define the requirements for the use of ISAs?	👍Yes 👎No
3.2.1	Are ISA templates available for standardizing ISA development?	👍Yes 👎No
3.2.2	Are your agencies ISAs centrally managed (recorded and filed)?	👍Yes 👎No

Data Domain Interoperability Objectives

The data domain encompasses the common identification, use, and sharing of data/information across the government. It provides guidance for consistently describing, categorizing, and sharing data and facilitates the discovery and exchange of information across boundaries. It describes structure (logical and schema) of the data/information at a level necessary for users to understand both what types of data/information is available and its structure. The data domain describes:

- Data classification and access management within a given data source by the mission or business context
- Storage and management of structured, semi-structured, and unstructured data used in a system
- Services and processes that reference or manipulate data
- Business context as applied to data to enable searches
- Standardization of information exchange (exchange models) between information sharing partners

Interoperability Objectives

Interoperability objectives of the data domain include:

- Describing how data is structured, what standards are used, how data/information can be exchanged to enable access and use
- Specifying/describing the data/information flow, including tagging, discovery, and retrieval of the data
- Defining routine exchanges
- Enabling data/information protection throughout the lifecycle
- Specifying how data/information is tagged/structured, and how specific data tagging standards are used
- Describing principles, roles, and responsibilities for data management and stewardship

Assessment

The Data Domain is divided into function or process groups. The review below provides an overall agency assessment of each group and several supporting questions. Please complete the below assessment.

	①: Ad-hoc	②: Repeatable	③: Enhanced	④: Managed	⑤: Optimized
Data Exchange	Business context is applied to the data Organization stores and manages defined, semi-defined, and undefined data for use by internal services and processes		Data is exchanged across agencies and missions in a standardized way		Data is exchanged across agencies and missions using open standards
Structural Metadata Definitions	The data structure is defined	Standards consistently define the data structure. Some automated data structuring and manual record-level tagging exists	A consistent, agency-adopted format with mostly automated structuring and manual record-level tagging of the data exists	Data tagging is semi-automated at the attribute-level with a community-adopted metadata format	Smart data tagged at the attribute-level with open metadata standards
Data Asset Discovery	Basic dataset-wide search capability exists	Basic system-wide search Business context is applied to the data so it is discoverable within the agency	Basic search of data assets that is configurable to federate from any system using a specific agency-adopted service contract	Advanced search of data assets that is configurable to federate from any system using a community-adopted service contract	Advanced search of data assets that is configurable to federate, is discoverable, available, and accessible across agencies and missions by using open standards
Exception Handling	No information is received from external organizations	Information is received but is unable to be stored or processed	Received information that is inconsistent with internal information exists is manually processed	Received information that is inconsistent with internal information is semi-automatically processed	Received information that is inconsistent with internal information is automatically processed

Security & Privacy	Security achieved through isolation of systems & implementing current regulatory mandates or laws	Supporting policies identified and under consideration	Supporting policies in process of development and implementation	Security is documented by consistent supporting policies, which are mostly implemented	Security is documented by consistent supporting policies, which are implemented

Data Domain Process		
1.0	**Overall Data Exchange**	①②③④⑤
1.1	Does your agency system that provide routine, automated, data exchanges?	👍Yes 👎No
1.2	Does you agency have a standardized process for developing and managing data models?	👍Yes 👎No
1.3	Does your agency have documented business requirements or rules/policies for mission-specific use cases?	👍Yes 👎No
1.4	Does your agency have common data standards for interoperability, including standards for vocabularies, ontologies, and models that represent the business information being exchanged?	👍Yes 👎No
2.0	**Overall Structural Metadata Definitions**	①②③④⑤
2.1	Does your agency have/use common standards, tags or attributes that support policies for managing data/information to be shared?	👍Yes 👎No
3.0	**Overall Data Asset Discovery**	①②③④⑤
3.1	Does your agency maintain a data asset catalog?	👍Yes 👎No
4.0	**Overall Exception Handling**	①②③④⑤
5.0	**Overall Security & Privacy**	①②③④⑤
5.1	Does your agency have documented privacy restrictions on data/information through the data lifecycle?	👍Yes 👎No
5.2	Does your agency have documented business requirements or rules/policies for mission-specific use cases?	👍Yes 👎No

Applications & Services Domain Objectives

The purpose of the applications and services domain is to describe the technical services supporting the common activities used for discovering, identifying, distributing, protecting, and managing the data/information needed by external users. It should:

- Provide any applicable service standards, application architecture approaches (e.g., SOA), or other information required to interact with the applications/services within the domain
- Describe the relationships between systems, applications, and interfaces

Interoperability Objectives

Interoperability objectives of the applications and services domain include:

- Capturing the specifications and functional requirements of the applications/services to the level necessary so external application developers can interface with applications/services
- Describing recommended and/or possible implementation approaches (e.g., cloud, SOA, mobile)
- Identifying services and common activities, their service components, and the interfaces/interconnections between the services and data assets that are exchanged
- Identifying the functions performed by the applications/services and any constraints on the data used and the flow of the data
- Specifying service standards used or required by the applications/services
- Specifying rules/laws with respect to products, data, and/or information generated by the applications/services
- Publishing/exposing application programming interfaces (APIs) so future users can access and create applications with the data/information, and describing how the developers access the APIs
- Describing extensibility approaches for future users/applications to add additional functionality
- Describing how application architecture scales for more users
- Describing how services are made discoverable
- Specifying the provider and user roles and responsibilities with respect to application/service lifecycle (from development to operations and maintenance, to retirement)

Assessment

The Applications and Services Domain is divided into function or process groups. The review below provides an overall agency assessment of each group and several supporting questions. Please complete the below assessment.

	①: Ad-hoc	②: Repeatable	③: Enhanced	④: Managed	⑤: Optimized
Business Service Models	Formalized business service models that depict information flows, relationships, and dependencies between services are not defined	Business service models are defined by a modeling standard and are aligned to applicable policy, guidance, and laws The models employ repeatable exchange patterns	The formalized business service models are understood by external partners, interoperable, and can be manually provided to authorized users	The formalized business service models are available online to authorized users	The formalized business service models are available online to authorized users
Service Discovery	Service is not discoverable	Service has undergone agency publication process, and is discoverable and accessible within the agency	Service is discoverable by all authorized users	Service is discoverable and accessible by authorized external users	Service is discoverable and accessible by authorized external users through an online repository
Service Delivery Method	Data exchange occurs physically, by telephone, or by email	Data is exchanged by a system-specific service with mostly automated pushes and pulls	Data is exchanged through an agency-wide service with entirely automated pushes and pulls	The method of data exchange is configurable to operate with any system using a community-adopted proprietary format with entirely automated pushes and pulls	The method of data exchange is configurable to operate with any system using an open standard with entirely automated pushes and pulls

Service-Level Agreements (SLAs)	No SLA The data is exchanged manually with external end users—may be governed by informal agreement	No SLA The data is exchanged manually with external end users—may be governed by informal agreement	No SLA Push-pull mechanism is loosely governed by an informal agreement that outlines expectations of a data exchange	The SLA exists and includes requirements for service availability, serviceability, performance, operation, as well as the roles and responsibilities between the service provider and service consumer to deliver and maintain the service. The SLA is not monitored	The SLA includes the standard/specification that addresses any interoperability considerations or constraints that affect implementation of the services Compliance monitoring of the SLA is automated

Applications & Services Domain Process		
1.0	**Business Service Models**	①②③④⑤
1.1	Does your agency publish/expose application programming interfaces (APIs)?	👍Yes 👎No
2.0	**Service Discovery**	①②③④⑤
2.1	Does your agency have a standard process for registering services?	👍Yes 👎No
3.0	**Service Delivery Method**	①②③④⑤
3.1	Does your agency employ user/client generated service request services?	👍Yes 👎No
3.2	Does your agency employ automated machine to machine services?	👍Yes 👎No
4.0	**Service-Level Agreements (SLAs)**	①②③④⑤
4.1	Does your agency execute SLA’s for data sharing?	👍Yes 👎No

Security Domain Interoperability Objectives

The purpose of security domain is to describe the security policies and considerations required for external users that need to interface and get access to the data/information. This domain typically:

- Ensures traceability between organizational or national level security policies and application level controls
- Provides the necessary security controls to ensure the protection of data/information as it is exchanged within and across security fabrics
- Pervades all of the other five domains because security and privacy controls need to be built into service workflows, data flows, systems, applications, and host networks
- Highlights how security considerations should also be captured and integrated into each domain, not considered at the end of an architecture or system development effort
- Leverages organizational policy to classify security controls for a segment or solution based on the type of information being processed

Interoperability Objectives

Interoperability objectives of the security domain include:

- Describing how proper security controls are used by the architecture to ensure data/information protection and allow access by external users
- Describing high-level security needs from an interoperability perspective, such as the use of common security standards/protocols
- Identifying controls required for specific types of information and any handling caveats (i.e., address confidentiality, integrity, and availability requirements)
- Describing how proper security controls are used to ensure data protection and ensure access
- Determining if information must be exchanged across different security enclaves
- Using metadata to tag data and describe its pedigree, lineage, source, timeliness, confidence, or other attributes associated with trust
- Identifying digital security rules, guidelines, and standards for securely exchanging data and services across security domains
- Describing, with enough detail for an external application developer, the event trace of the interactions of the architecture with regard to security controls
- Describing the identity management system used to allow/deny access to the data/information (i.e., role or attribute based)
- Describing the plan to manage/control your identity accounts and provide access controls to systems (for users, system administrators, developers, and super users)

- Describing how new users/developers are granted access to the data/information at all stages of the lifecycle
- Describing data/information access audit methods or standards, include the lifecycle for the storage of the audit data

Assessment

The Security Domain is divided into function or process groups. The review below provides an overall agency assessment of each group and several supporting questions. Please complete the below assessment.

	①: Ad-hoc	②: Repeatable	③: Enhanced	④: Managed	⑤: Optimized
Access Controls	Access controls do not exist or are physical	System-wide data access based on system-specific access categories with little automation of security inheritance	Record -level access based on agency-wide access categories with some automated security inheritance	Attribute-level access based on community-wide access categories with automated security procedures	Attribute-level access based on open standards for access categories, high flexibility in assigning credentials, and automated security procedure

Access/Security Domain Process		
1.0	**Access Controls**	①②③④⑤
1.1	Does your agency identify controls required for specific types of information and any handling caveats (i.e., address confidentiality, integrity, and availability requirements)?	👍Yes 👎No
1.2	Does your agency describe how proper security controls are used to ensure data protection and access?	👍Yes 👎No
1.3	Does your agency use metadata to tag the data and describe its pedigree, lineage, source, timeliness, confidence, or other attributes associated with trust?	👍Yes 👎No
1.4	Does your agency identify digital security rules, guidelines, and standards for securely exchanging data and services across security domains?	👍Yes 👎No
1.5	Does your agency develop, with enough detail for application developers, sequence diagrams describing system and security interactions?	👍Yes 👎No
1.6	Does your agency employ a common identity management system to allow/deny access to the data/information (i.e., role or attribute based)?	👍Yes 👎No
1.7	Does your agency audit data sharing transactions to monitor data use/movement?	👍Yes 👎No

Performance Domain Interoperability Objectives

The purpose of the performance domain is to provide linkage to investments or activities and an organization's strategic vision. This domain typically:

- Provides a direct line of sight between strategic planning and the investment review process
- Identifies common performance elements across investments or activities
- Provides a high-level overview of recommended metrics to be considered that will measure the successes of the architecture (inputs, outputs, and outcomes)

Interoperability Objectives

Interoperability objectives of the performance domain include:

- Define performance goals that align to applicable policy, guidance and laws[1]
- Review investments and ensure they clearly incorporate interoperability requirements and adhere to relevant performance goals[2]

[1] Within the ISE, specific reference should be given to incorporating responsible information sharing goals and objectives as defined by the National Strategy for Information Sharing and Safeguarding

[2] The ISE Performance Management Framework provides guidance on aligning vision, investment activities and metrics for responsible information sharing

Assessment

The Performance Domain is divided into function or process groups. The review below provides an overall agency assessment of each group and several supporting questions. Please complete the below assessment.

	➀: Ad-hoc	➁: Repeatable	➂: Enhanced	➃: Managed	➄: Optimized
Metrics	Formalized performance metrics that provide direct line of sight between strategic planning and the investment review process do not exist	Formalized performance metrics with goals that align to applicable policy, guidance, and laws exist	Formalized performance metrics that identifies common performance elements across investments or activities exists		Formalized performance metrics enable review of investments to determine if they incorporate interoperability requirements and adhere to relevant performance goals

Performance Domain Process		
1.0	**Metrics**	① ② ③ ④ ⑤
1.1	Does your agency maintain a performance reference model or metrics?	👍Yes 👎No
1.2	Does your agency describe the relationship between investments and their alignment with interoperability performance goals and how to measure the effectiveness of the investments	👍Yes 👎No
1.3	Does your agency evaluate current year performance measurement results to inform future year budget/investment decisions?	👍Yes 👎No

Appendix A: National MDA Architecture

The National MDA Architecture plan defines the Maritime Information Sharing Environment (MISE) as the platform for trusted sharing of information. The MISE provides a set of REST XML web services which utilize the National Information Exchange Model (NIEM) Maritime standard for common data representation. The MISE uses the *Trust Fabric* in conjunction with Attribute Based Access Control to manage and secure all data that flows through the MISE. The Trust Fabric defines the set of *Trusted Systems* who can share data via the MISE.

Trusted Systems

Within the MISE, every participating system is a "trusted system". A trusted system must have the ability to:

- Establish a SSL connection to the MISE, i.e. authenticate to the MISE via digital certificate and validate the certificate of the MISE server
- Issue, protect, manage user identities and associate security attributes to users,
- Generate SAML assertions that accurately assert attributes about the trusted system and users of that trusted system,
- Support XML and RESTful web services

The following questions will provide the required information to determine the level of "trust", and thus the level of access, of a trusted system.

System Level Controls		
1.0	Can your system use web services to exchange information?	👍Yes 👎No
2.0	Can your system use a SSL certificate to establish a secure connection?	👍Yes 👎No
3.0	Does your system manage information access to (un)authorized users?	👍Yes 👎No
4.0	Does your system manage user accounts/identities?	👍Yes 👎No
5.0	Can your system assign and manage user attributes?	👍Yes 👎No
6.0	Does your system have a process for account management to ensure the timely deletion or modification of user identities/attributes should a user's status change?	👍Yes 👎No
7.0	Does your system capture logs necessary to reconstruct the activities of authorized or unauthorized activities on the system	👍Yes 👎No

Attributes

Attributes are used to determine the data to which a user or system will be granted access. For the EXERCISE, a combination of the MISE Attributes and DHS attributes will be applied. They include:

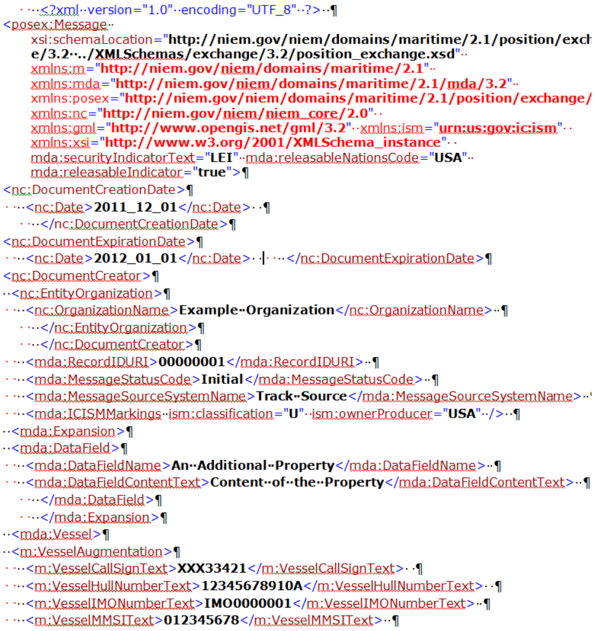
Indicator	
Law Enforcement Sensitive	LEI
Privacy Protected	PPI
Protected Critical Infrastructure Information	PCII
Sensitive But Unclassified	SBU
Federal/State/Local/Tribal/Territorial	FSLT
Community of Interest	COI
Private Sector Only	PSO
Nation (What nations *can* receive the data)	
Releasable (Is it publicly releasable)	

The following questions will be used to determine which attributes are assigned to your system.

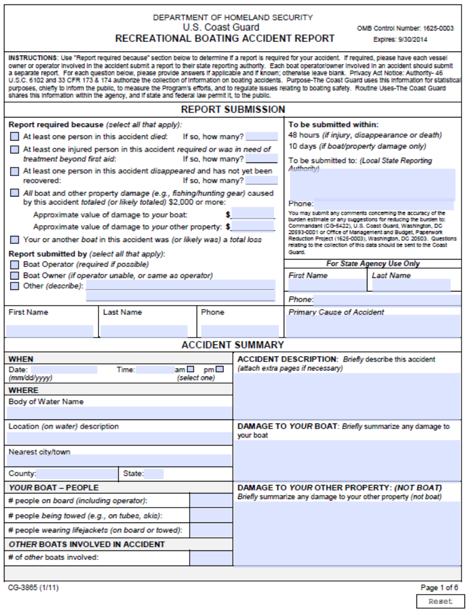
Attribute		
1.0	Does your department/agency/system manage LE data?	👍Yes 👎No
2.0	Does your department/agency/system manage PPI data?	👍Yes 👎No
3.0	Does your department/agency/system manage PCII data?	👍Yes 👎No
4.0	Does your department/agency/system manage SBU data?	👍Yes 👎No
5.0	Does your department/agency/system a PRI system?	👍Yes 👎No
6.0	What is the nationality of the system users?	USA CAN
7.0	Which Federal department or agency does your system represent?	______________
8.0	Which State department or agency does your system represent?	______________
9.0	Which Local department or agency does your system represent?	______________
10.0	Which Tribal department or agency does your system represent?	______________
11.0	Which Territorial department or agency does your system represent?	______________

Appendix B: Sample Messages

Samples of each message type that would be used to support the exercise will be required. While a sample of the actual message would be helpful, any message of that type will be useful. The message will be used to map to maritime data standards and provide the potential consumers an example of the data that could be provided.



```
  · ··<?xml··version="1.0"··encoding="UTF_8"··?>··¶
<posex:Message··
    xsi:schemaLocation="http://niem.gov/niem/domains/maritime/2.1/position/exch
    e/3.2··../XMLSchemas/exchange/3.2/position_exchange.xsd"··
    xmlns:m="http://niem.gov/niem/domains/maritime/2.1"··
    xmlns:mda="http://niem.gov/niem/domains/maritime/2.1/mda/3.2"··
    xmlns:posex="http://niem.gov/niem/domains/maritime/2.1/position/exchange/
    xmlns:nc="http://niem.gov/niem/niem_core/2.0"··
    xmlns:gml="http://www.opengis.net/gml/3.2"··xmlns:ism="urn:us:gov:ic:ism"··
    xmlns:xsi="http://www.w3.org/2001/XMLSchema_instance"··
    mda:securityIndicatorText="LEI"··mda:releasableNationsCode="USA"··
    mda:releasableIndicator="true">¶
<nc:DocumentCreationDate>¶
· ···<nc:Date>2011_12_01</nc:Date>··¶
  · ···</nc:DocumentCreationDate>¶
<nc:DocumentExpirationDate>¶
· ···<nc:Date>2012_01_01</nc:Date>··|· ···</nc:DocumentExpirationDate>¶
<nc:DocumentCreator>¶
··<nc:EntityOrganization>¶
· ···<nc:OrganizationName>Example··Organization</nc:OrganizationName>··¶
  · ···</nc:EntityOrganization>¶
  · ···</nc:DocumentCreator>¶
· ···<mda:RecordIDURI>00000001</mda:RecordIDURI>··¶
· ···<mda:MessageStatusCode>Initial</mda:MessageStatusCode>··¶
· ···<mda:MessageSourceSystemName>Track··Source</mda:MessageSourceSystemName>··
· ···<mda:ICISMMarkings··ism:classification="U"··ism:ownerProducer="USA"··/>··¶
··<mda:Expansion>¶
··<mda:DataField>¶
· ···<mda:DataFieldName>An··Additional··Property</mda:DataFieldName>··¶
· ···<mda:DataFieldContentText>Content··of··the··Property</mda:DataFieldContentText>··¶
  · ···</mda:DataField>¶
  · ···</mda:Expansion>¶
··<mda:Vessel>¶
··<m:VesselAugmentation>¶
· ···<m:VesselCallSignText>XXX33421</m:VesselCallSignText>··¶
· ···<m:VesselHullNumberText>12345678910A</m:VesselHullNumberText>··¶
· ···<m:VesselIMONumberText>IMO0000001</m:VesselIMONumberText>··¶
· ···<m:VesselMMSIText>012345678</m:VesselMMSIText>··¶
```



DEPARTMENT OF HOMELAND SECURITY
U.S. Coast Guard
RECREATIONAL BOATING ACCIDENT REPORT

OMB Control Number: 1625-0003
Expires: 9/30/2014

INSTRUCTIONS: Use "Report required because" section below to determine if a report is required for your accident. If required, please have each vessel owner or operator involved in the accident submit a report to their state reporting authority. Each boat operator/owner involved in an accident should submit a separate report. For each question below, please provide answers if applicable and if known; otherwise leave blank. Privacy Act Notice: Authority- 46 U.S.C. 6102 and 33 CFR 173 & 174 authorize the collection of information on boating accidents. Purpose-The Coast Guard uses this information for statistical purposes, chiefly to inform the public, to measure the Program's efforts, and to regulate issues relating to boating safety. Routine Uses-The Coast Guard shares this information within the agency, and if state and federal law permit it, to the public.

REPORT SUBMISSION

Report required because *(select all that apply)*:

□ At least one person in this accident *died*: If so, how many? ______

□ At least one injured person in this accident *required or was in need of treatment beyond first aid*: If so, how many? ______

□ At least one person in this accident *disappeared* and has not yet been recovered: If so, how many? ______

□ *All* boat and other property *damage (e.g., fishing/hunting gear)* caused by this accident *totaled (or likely totaled)* $2,000 or more:

Approximate value of damage to *your* boat: $______

Approximate value of damage to *your* other property: $______

□ Your or another *boat* in this accident was *(or likely was)* a *total loss*

Report submitted by *(select all that apply)*:

□ Boat Operator *(required if possible)*

□ Boat Owner *(if operator unable, or same as operator)*

□ Other *(describe)*: ______

To be submitted within:

48 hours *(if injury, disappearance or death)*

10 days *(if boat/property damage only)*

To be submitted to: *(Local State Reporting Authority)*

Phone:

You may submit any comments concerning the accuracy of the burden estimate or any suggestions for reducing the burden to: Commandant (CG-5422), U.S. Coast Guard, Washington, DC 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0003), Washington, DC 20503. Questions relating to the collection of this data should be sent to the Coast Guard.

For State Agency Use Only

First Name	*Last Name*

Phone:

First Name	Last Name	Phone	*Primary Cause of Accident*

ACCIDENT SUMMARY

WHEN

Date: ______ *(mm/dd/yyyy)* Time: ______ am □ pm □ *(select one)*

WHERE

Body of Water Name

Location *(on water)* description

Nearest city/town

County: ______ State: ______

***YOUR* BOAT – PEOPLE**

people *on board (including operator)*:

people *being towed (e.g., on tubes, skis)*:

people *wearing lifejackets (on board or towed)*:

***OTHER* BOATS INVOLVED IN ACCIDENT**

of *other* boats involved:

ACCIDENT DESCRIPTION: *Briefly* describe this accident *(attach extra pages if necessary)*

DAMAGE TO *YOUR* BOAT: *Briefly* summarize any damage to your boat

DAMAGE TO *YOUR* OTHER PROPERTY: *(NOT BOAT)* *Briefly* summarize any damage to your other property *(not boat)*

CG-3865 (1/11)

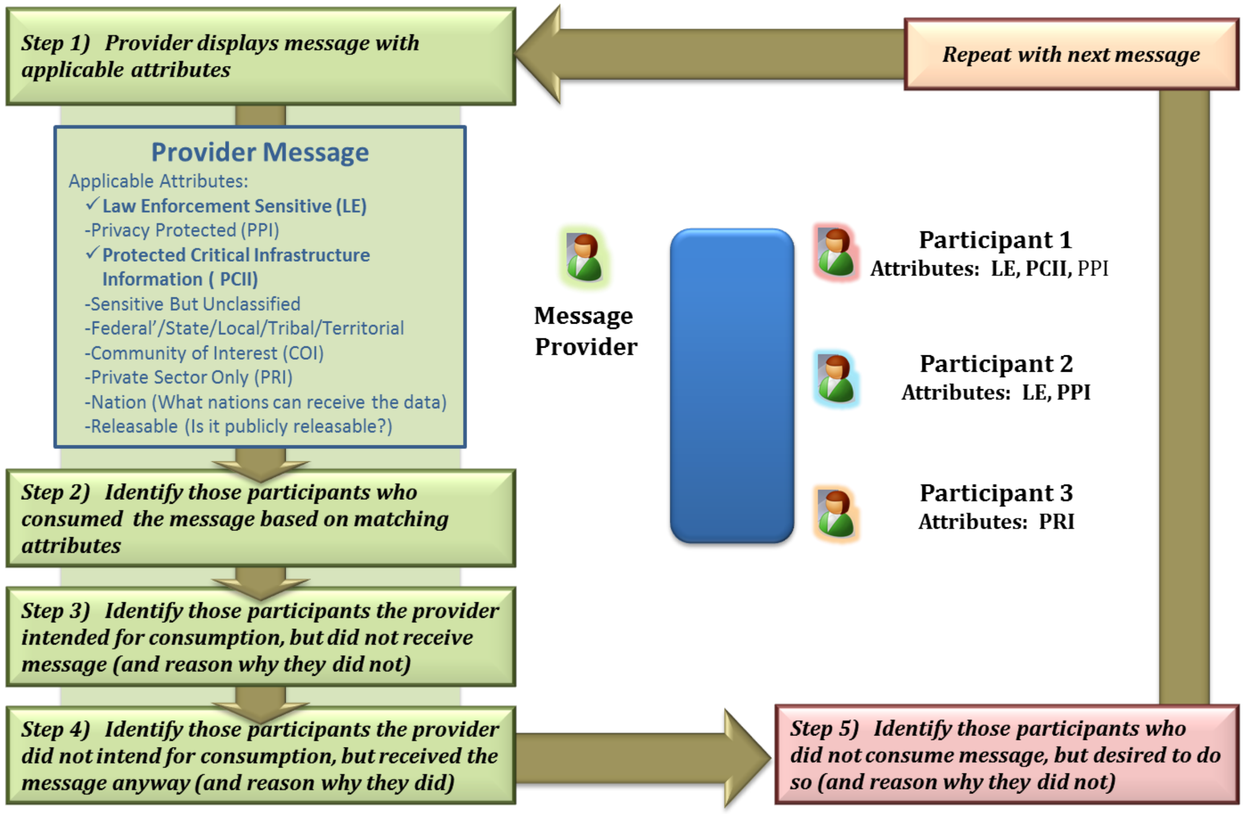
Page 1 of 6

Reset

Attributes	
LEI	👍Yes 👎No
PPI	👍Yes 👎No
PCII	👍Yes 👎No
SBU	👍Yes 👎No
FSLT	F/S/L/T:______________________________
COI	👍Yes 👎No
PSO	👍Yes 👎No
Nation	□ United States □ Canada
Releasable	👍Yes 👎No

Appendix C: Process Diagram

The preparation by the exercise team will be extensive to ensure a smooth and successful exercise. The below figure outline the steps that will be executed for each message to ensure there is complete understanding about who will and will not get the message and, as applicable, why.



Step 1) Provider displays message with applicable attributes

Provider Message

Applicable Attributes:

- ✓ **Law Enforcement Sensitive (LE)**
- -Privacy Protected (PPI)
- ✓ **Protected Critical Infrastructure Information (PCII)**
- -Sensitive But Unclassified
- -Federal'/State/Local/Tribal/Territorial
- -Community of Interest (COI)
- -Private Sector Only (PRI)
- -Nation (What nations can receive the data)
- -Releasable (Is it publicly releasable?)

Step 2) Identify those participants who consumed the message based on matching attributes

Step 3) Identify those participants the provider intended for consumption, but did not receive message (and reason why they did not)

Step 4) Identify those participants the provider did not intend for consumption, but received the message anyway (and reason why they did)

Step 5) Identify those participants who did not consume message, but desired to do so (and reason why they did not)

Repeat with next message

Appendix D: Participant Card

The participant card will provide information about each participant and the department/agency and system they are representing. The card will also contain the associated security attributes. The following is an example of the Participant card.

Representative: Jon Doe

Department: Department of Homeland Security

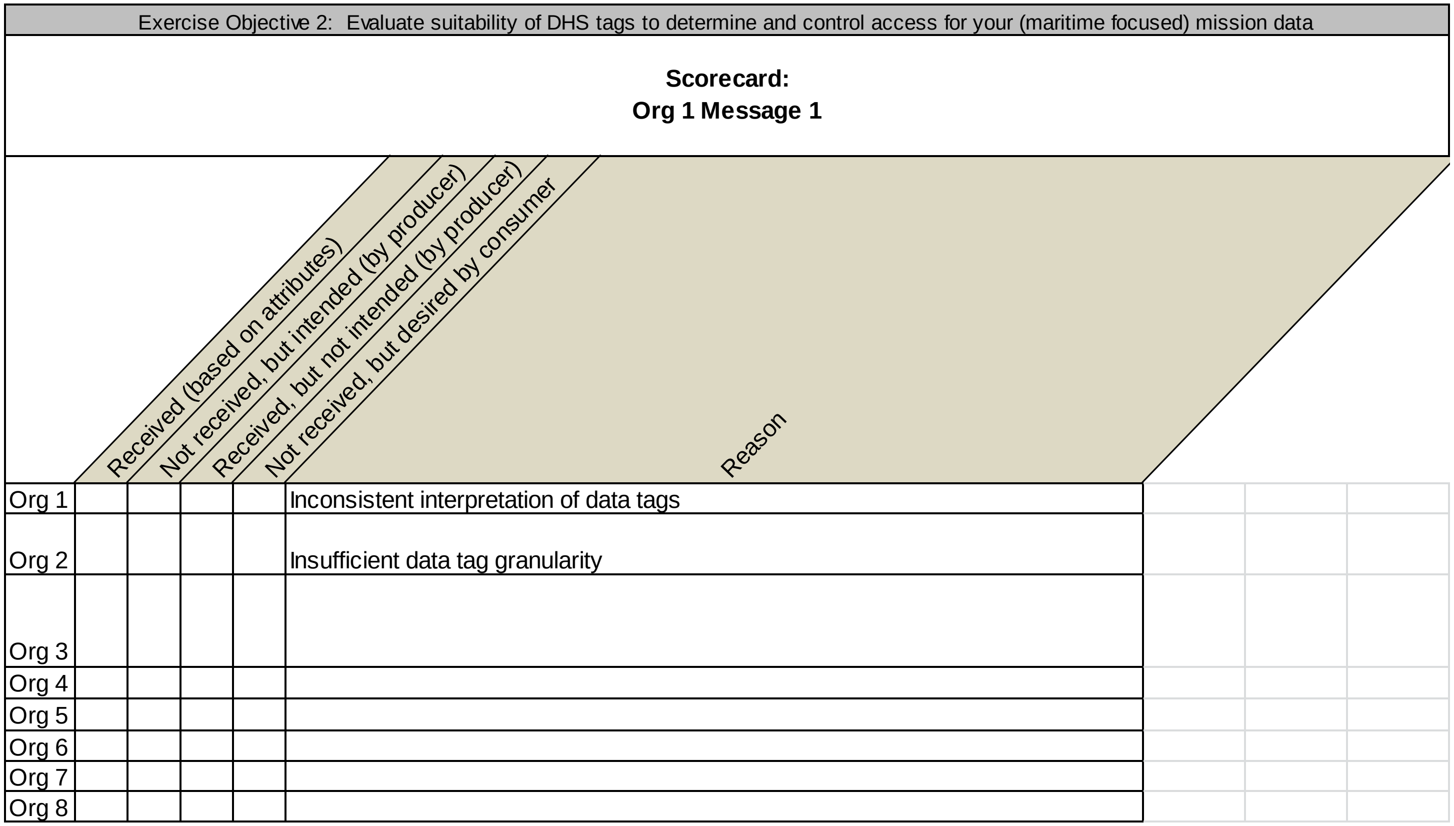
Agency: Coast Guard

System: Maritime Awareness Global Network (MAGNet)

Attributes	
LEI	👍Yes
PPI	👍Yes
PCII	👎No
SBU	👍Yes
FSLT	F: DHS
COI	👍Yes
PSO	👎No
Nation	United States

Appendix E: Sharing Score Sheet

A Sharing Score Sheet will be developed for each message that is used in the EXERCISE. It will allow recorders to capture the applicability of the attributes for the message and the distribution (sharing) of that message among participants. The following is an example of the Sharing Score Sheet.



Exercise Objective 2: Evaluate suitability of DHS tags to determine and control access for your (maritime focused) mission data

Scorecard:
Org 1 Message 1

	Received (based on attributes)	Not received, but intended (by producer)	Received, but not intended (by producer)	Not received, but desired by consumer	Reason
Org 1					Inconsistent interpretation of data tags
Org 2					Insufficient data tag granularity
Org 3					
Org 4					
Org 5					
Org 6					
Org 7					
Org 8					

Appendix F: Exercise Development Principals

Planning and Scope:	ISA IPC IISC, PM-ISE, and MDA Staff		
Document Development:	PM-ISE Staff		
Maturity Matrix Development:	PM-ISE Staff		
MDA Scenario and Document Foreword:	MDA Staff		
Exercise Coordinators:	Meghan Roberts	meghanlr@dni.gov	202-331-4085
	Sean Tweed-Kent	stweed@nmic.navy.mil	301-669-3164
	Frank Sisto	frank.sisto@navy.mil	703-614-1735
	Benjamin Berman	benjamin.berman.ctr@navy.mil	703-614-1767