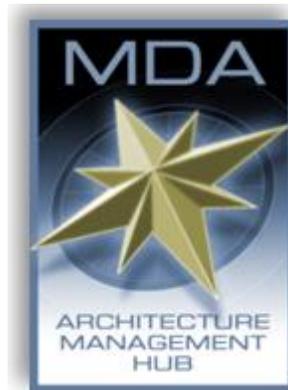

APPENDIX B - ATTRIBUTE SPECIFICATION



Maritime Information Sharing Environment (MISE)

Attribute Specification

Version 1.0

25 March 2013

1. Introduction

Maritime security is a national priority that depends on the ability to efficiently, effectively, and appropriately share and safeguard information among trusted maritime partners within the Global Maritime Community of Interest (GMCOI). The Maritime Information Sharing Environment (MISE) as defined in the National Maritime Architecture Plan enables secure, standardized sharing of unclassified maritime information among a wide variety of federal, state and local agencies as well as international participants. MISE employs attribute-based access control and a standardized set of security attributes for information access policy enforcement to facilitate information sharing with non-provisioned users in a dynamic environment. This security model embraces the philosophy that user accounts are most effectively managed by a user's parent organization and exploiting existing user account verification, management, and revocation processes already in place. Allowing access using an individual's existing local user identity and password improves security by eliminating the requirement to create and maintain yet another user identity. The federated model also eliminates the need for changes to user account privileges across multiple systems; an individual need only advise their parent organization of changes in employment status or organizational role, and changes to account privileges at the local level are sufficient to ensure security across the MISE domain. By federating the identity management to the trusted systems, the cost and burden of managing user accounts is greatly reduced for the MISE thus reducing overall sustainment costs. A common set of security attributes for entities, users, and data is necessary to consistently share and protect information across the federation of systems in the MISE.

1.1. PURPOSE

This specification defines a common set of attributes used within the Maritime Information Sharing Environment (MISE) to communicate information about users and the trusted systems that connect to the Information Sharing Infrastructure (ISI) on the user's behalf.

There are three categories for attributes defined for the National MDA Architecture:

1. Entity Attributes: Attributes that pertain to a trusted system within the MISE.
2. User Attributes: Attributes that pertain to a human user.
3. Data Attributes: Attributes that pertain to data.

Figure 1 summarizes the entity, user, and data attributes defined for the MISE.

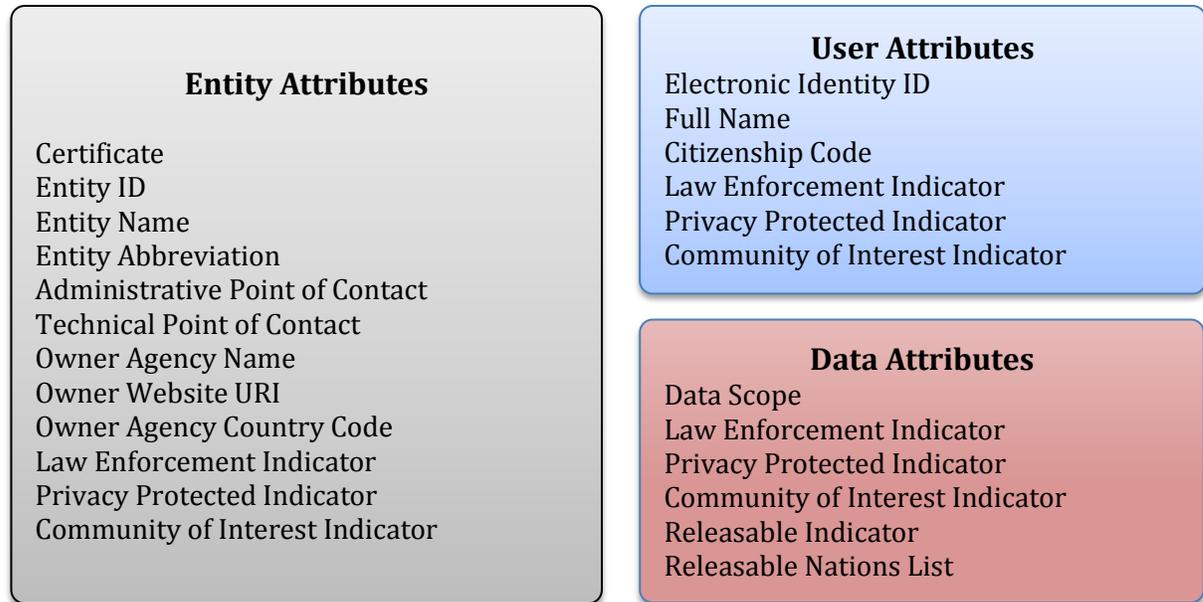


Figure 1 - MISE Attributes Summary

Entity attributes are used to capture relevant information about the trusted system i.e. SSL certificate, administrative information, and website Uniform Resource Identifier (URI). The Owner Agency Country Code is used in protecting data based on nation. An entity is restricted from accessing information unless it is explicitly coded for release to their country code. The "Indicator" attributes are key to establishing what categories of information the trusted system can access.

User attributes provide detailed information on the individual users of a trusted system, and serve to ensure that they are only able to access that subset of the available information to which they individually require and qualify for access. The user attributes are assigned and managed by the trusted system to which the user belongs.

Data attributes are fundamental to entitlement management and data management processes within the MISE. The three data attributes defined in this specification as “indicators” support entitlement management within the MISE. The “scope” attribute provides the flexibility to associate data with a specific incident or operation to provide context for data management.

1.2. INDICATORS

Entitlement management within the MISE involves run-time authorization decisions about whether a trusted system and requesting user are authorized to access a requested information resource. Three primary security indicators are used by data providers to declare information access policy to set access restrictions on information they share with MISE. These information access policies are the basis for entitlement decisions within the MISE. A fourth indicator, the “Releasable Indicator”, is a Boolean used in conjunction with the three primary Security Indicators to mark data as releasable to the public domain under the restrictions of the associated indicator. The three primary security indicators are listed in the following table in order of decreasing degree of restriction.

Indicator	Abbreviation
Law Enforcement	LEI
Privacy Protected	PPI
Protected Critical infrastructure Information	PCII
Sensitive but Unclassified	SBU
Federal State Local and Tribal	FSLT
Private Sector Only	PSO
Community of Interest	COI

Table 1 – Security Indicators

The following describes the three primary attributes and explains their intent as well as how the attribute might be used:

Law Enforcement Indicator: This Indicator is the most restrictive, and is used to code data for release to entities such as federal, state and local law enforcement agencies. Only Entities assigned the Law Enforcement Indicator and the U.S. owner agency code can access this data. Within an Entity with the Law Enforcement Indicator, only Users who are U.S. Citizens and assigned the Law Enforcement Indicator by that Entity will be able to access the information.

Privacy Protected Indicator: Personally Identifiable Information (PII) is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. State and Federal legislation, as well as the policy of many agencies such as DOD and DHS, impose strict limitations on the release of PII. The Privacy Protected Indicator is designed to restrict access to and distribution of PII across the MISE Domain. Application of the Privacy Protected Indicator means the information will only be released to Entities with the requisite country code, and then only to Individuals with that attribute and the requisite country code assigned to their account.

Protected Critical Infrastructure Information: Protected Critical Infrastructure Information Indicator (PCII) Communities are responsible for protecting national/state identified critical infrastructure facilities. Critical infrastructure information means information not customarily in the public domain and related to the security of criminal infrastructure or protected systems.

Sensitive but Unclassified: Non PPI, non LEA information that is not publically releasable. Sensitive but Unclassified is an indicator category of information that requires protections against discloser. This security indicator limits the discloser of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.

Federal, State, Local, & Tribal: Defines the level of government authorized to receive information. Information limited to jurisdictional boundaries, or that is partitioned to specific geographic area, depending on resources and limitations.

Private Sector Only: Private Sector Only is an indicator that protects commercial and proprietary interest. Information cannot be redistributed to other entities due to the enclosed information and is only intended for authorized disclosures.

Community of Interest Indicator: The community of interest indicator is the minimum access level assigned to trusted systems participating in the environment. By default, all trusted systems are granted the Community of Interest Indicator.

The following two modifiers can be used in conjunction with any of the three primary security indicators:

Releasable Indicator (default False): This attribute is a Boolean value to mark data as releasable to the public domain under the restrictions of the associated indicator. This attribute is used to indicate data can be released in accordance with the consuming systems policies, business processes and as required to support their mission.

Releasable Nations List (default USA): This provides a comma-separated list of nations who can access the associated data. This is a space-separated list of three-letter country codes, for example (CAN USA FRA). This attribute is used to indicate data can be released to only those nations identified by country codes.

Scope provides tags to associate data with a specific incident or operation. These tags are used by data providers to relax or override their IAP for normal operations so trusted systems and users are able to access data they would normally be restricted from, but only within the scope of their involvement in the specified event or operation. Scope may be a planned event such as the Olympics or specific response operation in the wake of a specific disaster such as Hurricane Katrina. Each scope is named, and provides three modifiers to the data indicators discussed in the previous section:

ScopeName: Unique name of a scope. This will indicate which event or operation within which the scope is in context, e.g. SuperstormSandy.

ScopeIndicator: Minimum indicator required for access within the context of this scope. If this data is normally PPI data, the data provider might want to provide it to all COI consumers within the context of this scope.

ScopeReleasable: This attribute is a Boolean value to mark data as releasable to the public domain under the restrictions of the associated indicator. This attribute is used to indicate data is can be released in accordance with the consuming systems policies, business processes and as required to support their mission, within the context of the associated scope.

ScopeReleaseableNations: This provides a comma-separated list of nations who can access the associated data within the context of the associated scope. This is a space-separated list of three-letter country codes, for example (CAN USA FRA).

As an example, the following table shows in the case of a trusted system providing position reports, the policy during routine operations is PPI required for access because the data contains US Persons information. However, in support of disaster relief operations during Hurricane

Sandy the data provider may decide they have a need to share with any trusted system within the context of Humanitarian Aid and Disaster Relief (HADR) operations so COI can be set as minimum requirement for access. The data provider can modify the indicator, releaseability, and releasable nations in the context of the Hurricane Sandy scope only.

Use Case (Tracks)	Routine Operations	Indicator/Scope
HADR (US Persons)	PPI	COI / SuperstormSandy

Table 2 – Scope Example

The four attributes described for scope are not new attributes, but simply modifiers on the existing data attributes defined in Section 4 of this specification.

2. Entity Attributes

The following entity attributes are associated with a trusted system.

2.1 Administrative Point of Contact – Email Address Text	
Name	AdministrativePointofContactEmailAddressText
Description	The electronic mailing address by which to contact the person who is the administrative point of contact for the entity within the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:AdministrativePointofContactEmailAddressText
Example Values	“john.doe@company.com”
2.2 Administrative Point of Contact – Fax Number	
Name	AdministrativePointofContactFaxNumber
Description	The telephone number for a facsimile device by which to contact the person who is the administrative point of contact for the entity within the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification

Formal Name	gfipm:2.0:entity:AdministrativePointofContactFaxNumber
Example Values	“(555) 555-5555”
2.3 Administrative Point of Contact – Full Name	
Name	AdministrativePointofContactFullName
Description	The complete name of the person who is the administrative point of contact for the entity within the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:AdministrativePointofContactFullName
Example Values	“John Doe”
2.4 Administrative Point of Contact – Telephone Number	
Name	AdministrativePointofContactTelephoneNumber
Description	The telephone number for a telecommunications device by which to contact the person who is the administrative point of contact for the entity within the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:AdministrativePointofContactTelephoneNumber
Example Values	“(555) 555-5555”
2.5 Certificate	
Name	Certificate
Description	An electronic certificate used by the entity as a cryptographic trust anchor within a federation for the purposes of digital signatures and/or encryption. The certificate is represented in X.509 v3, base-64 encoded format.
Data Type	Base-64 Binary
Typical Usage	Authentication, Registration, Audit Logging
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:Certificate
Example Values	"MIICJzCCAZCgAwIBAgIBGDANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJVUzEMMAoGAIUEChMDSVNDMSMwIQYDVQQDExpJU0MgQ0RLIFNhbXBsZSBkZXJ0aWZl"

	pY2F0ZTAeFw0wMzA3MTcwMDAwMDBaFw0wNDA3MTc wMDAwMDBaMEAxCzAJBgNVBAYTAIVTMQwwCgYDVQ QKEwNjU0MxIzAhBgNVBAMTGklTQyBDREsgU2FtcGxllE NlcnRpZmljYXRlMIGfMA0GCSqGSIb3DQEBAQUAA4GNA DCBiQKBgQC9GQTkukn+153rATR8dh2Hm8ixF7f7Y7b10VFJ nJAQCKqta4/lhFwQIK5F2Gn8j9tITBiXCF7F6XSvaF8bivN10z R0pvI1lNflEm2kwh7Yw0jZJB17Y3FHgl83qYegmm/UwqX5zK Ua4xw+cE8XSEqUuwjg0roBMGhAMzFEihHzLwIDAQABoz EwLzAMBgNVHRMBAf8EAjAAMA4GAIUdDwEB/wQEAwI AYDAPBgNVHQ4ECHJzYS0xMDI0MA0GCSqGSIb3DQEBB QUAA4GBALWGxxo55ScpLfECnqEUixFwrzftQGD2ISda7E Wp/d7k23fOXgHC7Zal8OpvlBUZ3sC2Fg4finfRHd2J4mXON k5OEedjhJILd58GErcCECg4J2uJPz77/zk+giiXldQEPTG+YOaAb ZC2SFbdfyYDKiSPhgzyd0/b4cElf4+VzegRM"
2.6 Community of Interest Indicator	
Name	COIIndicator
Description	True if the entity is allowed access to COI data, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:entity:COIIndicator
Example Values	"True," "False"
2.7 Entity Abbreviation	
Name	EntityAbbreviation
Description	An abbreviation or acronym for the name of a trusted system.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:EntityAbbreviation
Example Values	"MAGNET," "MSSIS"
2.8 Entity ID	
Name	EntityID
Description	The unique identifier by which the entity is denoted.
Data Type	Text
Typical Usage	Registration, Audit Logging
References	GFIPM 2.0 Metadata Specification

Formal Name	gfipm:2.0:entity:EntityId
Example Values	“MSSIS:123,” “MISE:TIB:MAGNET”
2.9 Entity Name	
Name	EntityName
Description	The name of an entity.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:EntityName
Example Values	“Maritime Analysis Global Network,” “Maritime Safety and Security Information System”
2.10 Law Enforcement Indicator	
Name	LawEnforcementIndicator
Description	True if the entity is allowed access to law enforcement protected data, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:entity:LawEnforcementIndicator
Example Values	“True,” “False”
2.11 Owner Agency Country Code	
Name	OwnerAgencyCountryCode
Description	The country of the organization or agency by which the entity is owned and operated.
Data Type	Country Code ISO 3166-1
Typical Usage	Registration
References	
Formal Name	mise:1.4:entity:OwnerAgencyCountryCode
Example Values	“USA,” “GBR,” “FRA”
2.12 Owner Agency Name	
Name	OwnerAgencyName
Description	The name of the organization or agency by which the trusted

	system is owned.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:OwnerAgencyName
Example Values	"NORAD-USNORTHCOM"
2.13 Owner Agency Website URI	
Name	OwnerAgencyWebSiteURI
Description	The Internet address or website of the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:OwnerAgencyWebSiteURI
Example Values	"http://website.company.com"
2.14 Privacy Protected Indicator	
Name	PrivacyProtectedIndicator
Description	True if the entity is allowed access to privacy-protected data, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:entity:PrivacyProtectedIndicator
Example Values	"True," "False"
2.15 Technical Point of Contact – Email Address Text	
Name	TechnicalPointofContactEmailAddressText
Description	The electronic mailing address by which to contact the person who is the technical or engineering point of contact for the entity within the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:TechnicalPointofContactEmailAddressText

Example Values	“john.doe@company.com”
2.16 Technical Point of Contact – Fax Number	
Name	TechnicalPointofContactFaxNumber
Description	The telephone number for a facsimile device by which to contact the person who is the technical or engineering point of contact for the entity within the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:TechnicalPointofContactFaxNumber
Example Values	“(555) 555-5555”
2.17 Technical Point of Contact – Full Name	
Name	TechnicalPointofContactFullName
Description	The complete name of the person who is the technical or engineering point of contact for the entity within the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:TechnicalPointofContactFullName
Example Values	“John Doe”
2.17 Technical Point of Contact – Telephone Number	
Name	TechnicalPointofContactTelephoneNumber
Description	The telephone number for a telecommunication device by which to contact the person who is the technical or engineering point of contact for the entity within the organization or agency by which the entity is owned and operated.
Data Type	Text
Typical Usage	Registration
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:entity:TechnicalPointofContactTelephoneNumber
Example Values	“(555) 555-5555”

Table 3 – List of Entity Attributes

3. User Attributes

The following user attributes are associated with an end user.

3.1 Citizenship Code	
Name	CitizenshipCode
Description	The country that has assigned rights, duties, and privileges to the user because of the birth or naturalization of the user in that country.
Data Type	ISO 3166-1 Alpha-3 Country Code
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:user:CitizenshipCode
Example Values	"USA," "GBR," "FRA"
3.2 Community of Interest Indicator	
Name	COIIndicator
Description	True if the user is allowed access to COI data, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:user:COIIndicator
Example Values	"True," "False"
3.3 Electronic Identity Id	
Name	ElectronicIdentityId
Description	The unique identifier that is associated with the electronic identity for the user within the user's identity provider's user base.
Data Type	Text
Typical Usage	Audit Logging
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:user:ElectronicIdentityId
Example Values	"DOE.JOHN.A.2370295257"
3.4 Full Name	

Name	FullName
Description	The complete name of the user.
Data Type	Text
Typical Usage	Audit Logging
References	GFIPM 2.0 Metadata Specification
Formal Name	gfipm:2.0:user:FullName
Example Values	“John Doe,” “Jim Q. Public”
3.5 Law Enforcement Indicator	
Name	LawEnforcementIndicator
Description	True if the user is allowed access to law enforcement protected data, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:user:LawEnforcementIndicator
Example Values	“True,” “False”
3.6 Privacy Protected Indicator	
Name	PrivacyProtectedIndicator
Description	True if the user is allowed access to privacy-protected data, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:user:PrivacyProtectedIndicator
Example Values	“True,” “False”

Table
4 –
List of
User
Attributes

4. Data Attributes

The following data attributes are associated with information exchanged within the MISE.

4.1 Community of Interest Indicator	
Name	COIIndicator
Description	True if the data is COI protected, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:data:CommunityOfInterestIndicator
Example Values	“True,” “False”
4.2 Data Scope	
Name	Scope
Description	An indicator which denotes a scope, situation, or event of interest for which data is deemed relevant and/or accessible.
Data Type	Text
Typical Usage	Authorization
References	
Formal Name	mise:1.4:data:Scope
Example Values	“HurricaneKatrina,” “Baltimore1812Exercise,” “OperationTomadachi”
4.3 Law Enforcement Indicator	
Name	LawEnforcementIndicator
Description	True if the data is law enforcement-protected, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:data:LawEnforcementIndicator
Example Values	“True,” “False”
4.4 Privacy Protected Indicator	

Name	PrivacyProtectedIndicator
Description	True if the data is privacy-protected, false otherwise.
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:data:PrivacyProtectedIndicator
Example Values	“True,” “False”
4.5 Releasable Indicator	
Name	ReleasableIndicator
Description	True if the data is publicly releasable
Data Type	Boolean
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:data:ReleasableIndicator
Example Values	“True,” “False”
4.6 Releasable Nations	
Name	ReleasableNationsCodeList
Description	A space separated list of countries with assigned rights, duties, and privileges to access the data.
Data Type	ISO 3166-1 Alpha-3 Country Code
Typical Usage	Authorization, Audit Logging
References	
Formal Name	mise:1.4:data:ReleasableNationsCodeList
Example Values	”USA GBR FRA”

Table 5 – List of Data Attributes

VERSION 3.0
RELEASE 1
FEBRUARY 2015