

DEMONSTRATION 1

Information sharing through CISE

Including long term data preservation and creation of European Common Language of data

Speaker:

Patrice Lesueur

**Direction Nationale Garde-Côtes des Douanes,
France (DNGCD)**



**11-12 September
2024**



**ASI Headquarters
Via del politecnico snc,
00133 Roma (Italia)**

Information sharing through CISE

Long term data preservation and
creation of a European common
language of data



Authorities at Member State level carry out many different maritime surveillance tasks.

Activities in sectors like **maritime safety and security, fisheries control, marine environment, customs, border control, law enforcement and defence** all require up to real time information from different sources.

The common information sharing environment – CISE is a leap forward in sharing maritime surveillance data between different governmental communities with a responsibility at sea.



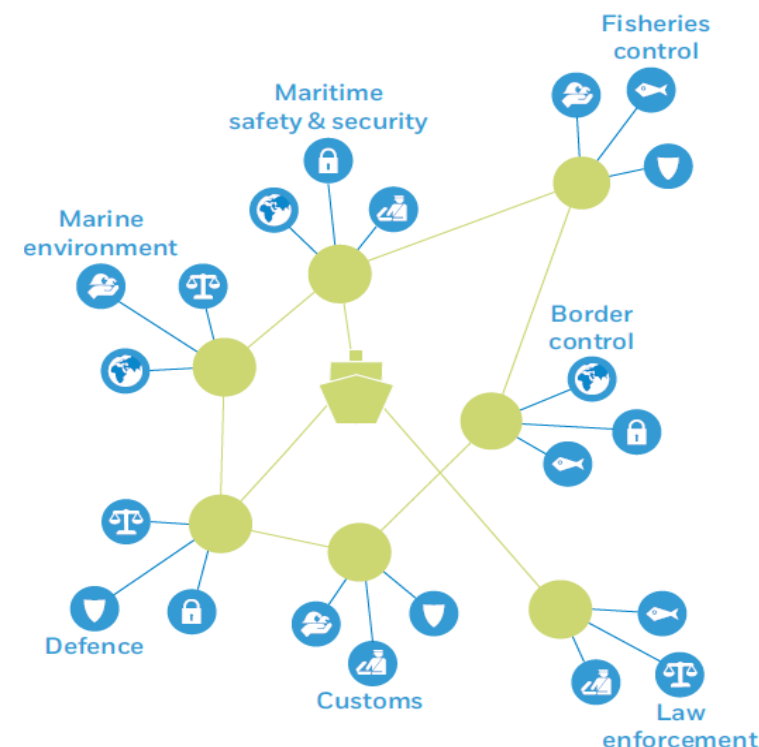
What is CISE?

CISE works via a **network of nodes** in member States and EU Agencies, which takes information from the various existing maritime surveillance systems.

It allows the exchange of **relevant information** across geographical boundaries and beyond usually closed sectors of activity such as safety, maritime security, fisheries control, border control, the fight against fraud, defence or the environment.

Joining CISE also implies signing **a cooperation agreement**, which defines the conditions of the safe use of the data shared.

In addition, Stakeholders should endorse **the responsibility to share** principle, which means they can use data that comes from CISE, but they have to provide data too.



Why CISE?

Member State authorities collect data and information through their sectoral platform and dedicated IT systems to obtain an improved picture.

But

Sharing information can be complex, useless and expensive: shared knowledge is only of interest to a limited extent.

In some cases, information are not even shared:

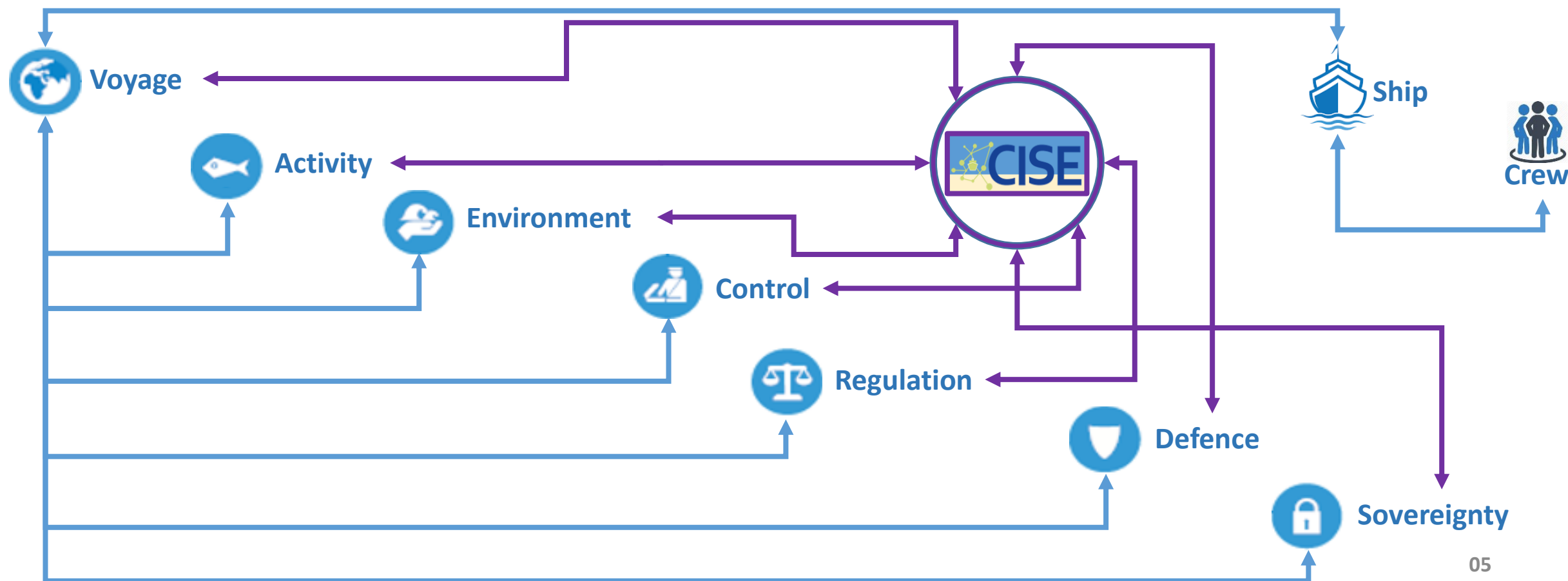
- 1** The authorities are not aware that useful information are available elsewhere or that they have information that is of interest to others.
- 2** There is no legal framework for sharing this type of information between authorities and agencies across Europe.



This can lead to data duplication or, on the contrary, a lack of data leading to unnecessary operational costs in one-off and laborious exchanges.

Purpose of CISE

Each agency of each MS stores maritime data, the interest of which varies according to the professions practiced. CISE facilitates and accelerates the process of information sharing by interconnecting EU maritime networks and Member States' surveillance systems.



Added value of CISE

- Low level Information stored by one maritime authority is potentially of high value and useful for another
- No additional system
- Full control over information
- Simpler operations management



To gather additional
information about a
maritime event



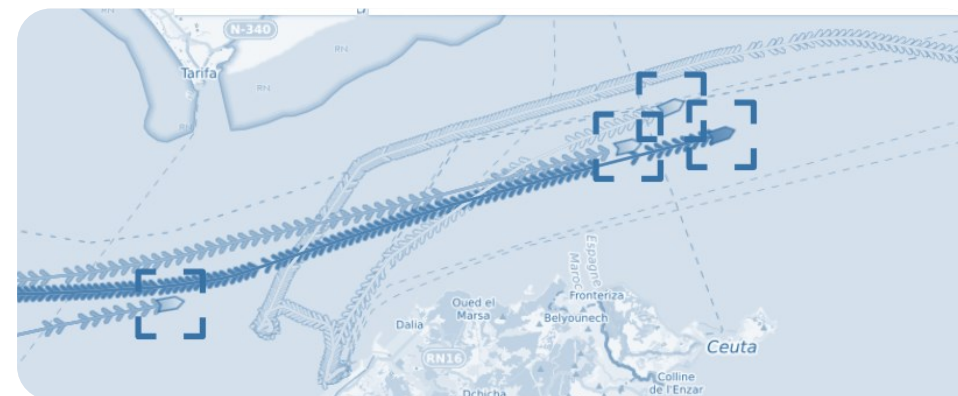
To request operational
assets, risk analysis,
former recording



Added value of CISE



Exchange of alerts on positions, behaviours



Exchange of documents, risk analysis, suspicious situation



A new ontology

The semantic representation of the CISE data model makes everyone agree on the large bag of classes...

Action	ActionPriorityType	ActionStatusType	ActionType	Agent	AgentAgent	AgentEvent	AgentLocation	AgentObject	AgentRisk
AgentRoleInAgentType	AgentRoleInEventType	AgentRoleInLocationType	AgentRoleInObjectType	AgentRoleInRiskType	Aircraft	Anomaly			
AnomalyType	AssociationClass	AttachedDocument	Cargo	CargoDocument	CargoDocumentType	CargoType	CargoUnit	Catch	CertaintyType
CertificateDocument	CertificateDocumentType	CloudCoverType	ColourType	CommunityStatusType	ConditionOfTheCargoAndBallastType				
ContainmentUnit	CorrelatedWith	CorrelationType	CrisisIncident	CrisisIncidentType	DangerousSubstancesType	Document	DutyType	Entity	
EnumerationType	Event	EventAreaType	EventDocument	EventDocumentType	EventEvent	EventLocation	EventRoleInEventType	FileMediaType	
FishingGearType	FormalOrganization	GenderType	Geometry	HullMaterialType	Incident	INFClassType	InformationReliabilityLevelType		
InformationSecurityClassificationType	InformationSensitivityDegreeType	IrregularMigrationIncident	IrregularMigrationIncidentType	ISO3166CountryCodeType					
ISPSSecurityLevelType	LandVehicle	LawInfringementIncident	LawInfringementIncidentType	Location	LocationDocument	LocationDocumentType			
LocationQualitativeAccuracyType	LocationRoleInEventType	LocationRoleType	LocationZoneType	MaritimeSafetyIncident	MaritimeSafetyIncidentType				
Metadata	MeteoOceanographicCondition	MetocType	MissionType	Movement	MovementType	NamedLocation	NatureType	NavigationalStatusType	
Object	ObjectEvent	ObjectLocation	ObjectRoleInEventType	OperationalAsset	OperationalAssetType	OperationalCapabilityType			
OperationalPurposeType	Organization	OrganizationalCollaboration	OrganizationalUnit	OrganizationClassificationType		OrganizationDocument			
OrganizationDocumentType	OrganizationPurposeType	OrganizationRoleType	PackageType	PackagingMaterialType	PackingGroupCodeType	Period			
Person	PersonDocument	PersonDocumentType	PersonIdentificationType	PersonIdentifier	PlacementPurposeType	PlannedOperationsType			
PlannedWorksType	PollutionCodeType	PollutionIncident	PollutionType	PortFacilityLocation	PortLocation	PortOrganization	Relationship		
ResponseType	Risk	RiskAgent	RiskDocument	RiskDocumentType	RiskLevelType	RiskProbabilityType	RiskSeverityType	RiskType	
SanitaryMeasureType	SeaConditionType	SensorType	SeverityType	ShipConfigurationType	SourceType	SpeciesType	Stream	StreamType	
TidesType	UNDGType	UniquelIdentifier	UnitsOfMeasureType	UrgencyType	Vehicle	Vessel	VesselDocument	VesselDocumentType	VesselType
WeatherConditionType	WeightMeansType								



... and the huge object properties.

hasActionActionStatus	hasActionActionType	hasActionMission	hasActionPriority	hasAgentAgentAgent	hasAgentAgentAgentRole	hasAgentAgentDuty
hasAgentAgentInvolvementPeriod	hasAgentDocument	hasAgentEventAgent	hasAgentEventAgentRole	hasAgentEventEvent		
hasAgentEventInvolvementPeriod	hasAgentIdentifier	hasAgentLocationAgent	hasAgentLocationAgentRole	hasAgentLocationInvolvementPeriod		
hasAgentLocationLocation	hasAgentMetadata	hasAgentObjectAgent	hasAgentObjectAgentRole	hasAgentObjectDuty	hasAgentObjectInvolvementPeriod	
hasAgentObjectObject	hasAgentRiskAgent	hasAgentRiskAgentRole	hasAgentRiskInvolvementPeriod	hasAgentRiskRisk	hasAnomalyAnomalyType	
hasCargoCargoType	hasCargoContainedCargoUnit	hasCargoDocumentDocumentType	hasCatchWeightMeans	hasCertificateDocumentDocumentType		
hasContainmentUnitCommunityStatusOfGoods	hasContainmentUnitDangerousSubstancesCode	hasContainmentUnitPackageType				
hasContainmentUnitPackagingMaterial	hasContainmentUnitPackingGroupCode	hasContainmentUnitPollutionCode	hasContainmentUnitUnitsOfMeasure			
hasCorrelatedWithCorrelatedBy	hasCorrelatedWithCorrelationType	hasCorrelatedWithUniquelIdentifier	hasCrisisIncidentCrisisIncidentType			
hasDocumentIdentifier	hasDocumentLocation	hasDocumentMetadata	hasEventDocument	hasEventDocumentDocumentType	hasEventEventEvent	
hasEventEventEventRole	hasEventEventInvolvementPeriod	hasEventIdentifier	hasEventLocationDateTime	hasEventLocationEvent		
hasEventLocationEventArea	hasEventLocationLocation	hasEventLocationLocationRole	hasEventLocationSourceType	hasEventMetadata		
hasEventNatureType	hasEventOccurrencePeriod	hasEventRisk	hasIncidentCertainty	hasIncidentResponseType	hasIncidentResponseUrgency	
hasIncidentSeverity	hasIrregularMigrationIncidentIrregularMigrationIncidentType					

Each maritime LS defines at least :
one “Cargo” class
&
one “Location” object

A new ontology

One example : The class Anomaly.

An anomaly is used to characterize an unusual event at sea which deserves to be noted or reported.

With CISE, it can relate to every type of anomaly that a standard legacy system could understand.



Document
Risk
Event
Period
Location
Agent

A new ontology

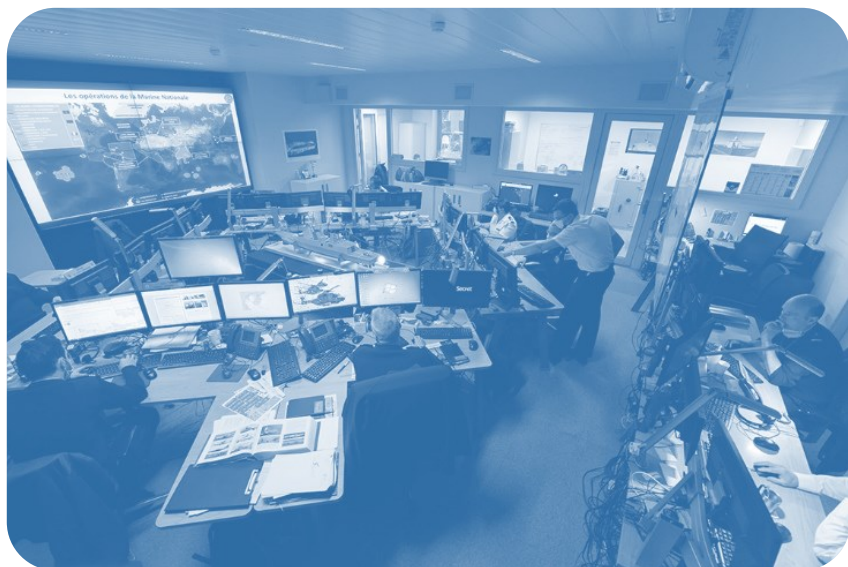
Universal grammar and spelling

Some “operational” services **End-users oriented**

Some CISE services “strictly speaking” : **Easy to choose and to aggregate**

Involved CISE protocols : **Push/pull/subscribe protocols to manage the flow**

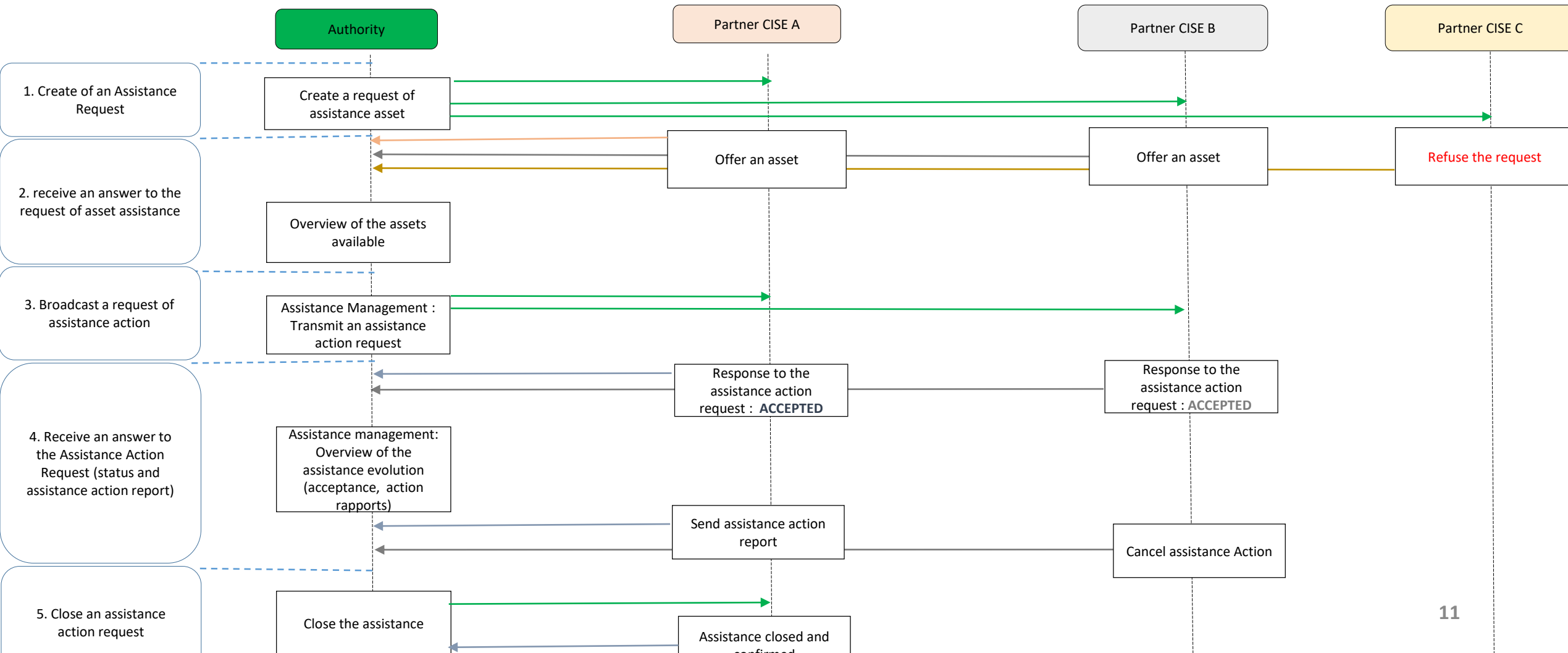
Involved attributes : to specify the information elements



SHALL WE PLAY A GAME



A clear process to request and submit



A European circle of trust based on security



Categories		
Security	Law enforcement	Regulation
Terrorism support	Prohibited imports – arms	Flag state, ownership, crew composition, previous port of call
Crew members/passengers with association with terrorists/terrorism	Prohibited imports - narcotics, illicit tobacco including precursor chemicals	first time in port of regulatory interest
Engaged in intelligence collection/history of suspicious activity	Migration - illegal immigration/human trafficking	History of regulatory non-compliance
	Serious organized criminal activity	dangerous cargo
	Exploitation of natural resources illegal, unreported, unregulated fishing	people/cargo with dangerous/infectious pathogens - agriculture
	Marine pollution	Invasive species
	Illegal activity of activist groups	unusual transit/operating in or transiting an environmentally sensitive area, exclusive zone, or restricted area
	General maritime security - piracy, violence, stateless vessels	Sanctions/UN security council resolution violations
	Migration - passport discrepancies	

Two networks : EU Restricted and EU Classified

As a reminder:

Built on cooperation and collaboration, CISE is at the heart of a constantly expanding network connecting legacy systems. It brings advanced technology and information sharing together for safer, more secure, more sustainable seas around Europe and beyond.

So, Let's share our maritime data.

Thanks a lot for your attention.

patrice.lesueur@douane.finances.gouv.fr

