ESSA
CREATE SHARE ENHANCE

ENHANCE SHARED SITUATIONAL AWARENESS

Information Sharing Architecture (ISA) Access Control Specification (ACS)

Supplement to the ISA Shared Situational Awareness (SSA)

Requirements Document

Version 3.0a
June 2019

https://www.us-cert.gov/essa

Record of Changes

Version	Date	Author	Changes
1.0	Aug 28, 2013	ISA Implementation Working Group	Initial publication.
1.1	Feb 10, 2014	ESSA Portfolio Management Team	• Editorial changes and clarifications • Updated some values in Appendix A to match or deconflict with US Agency values in IC EDH • Deleted Supplemental Sensitivity Criteria and replaced it with Source Entity • Added Resource Deletion Date and Time • Added ECS in Logical Access Criteria/Groups • Replaced ISA Participant with NCC (National Cyber Centers) in Logical Access Criteria/Groups • Added Appendices C & D to compare the ISA ACS and existing specifications • Limited the values of Dissemination Controls to those requested by the ISA Participants • Specified which CUI categories are needed by ISA Participants • Limited the "User Status" resource attribute values so they map directly to the "Entity Type" entity attribute • Added derived ISA requirements • Added Proprietary, Law Enforcement Sensitive (LES), and LES NOFORN to Dissemination Controls to match CAPCO • Changed Public Release Dissemination (True/False) to a required field for unclassified resources
2.0	December 16, 2014	ESSA Portfolio Management Team	• Incorporated major updates to Resource Attributes based on the creation of the ISA implementation of SD-EDH. • Made minor changes to user attributes based on resource changes. • Updated Use Cases in Section 5. Updated Organizational values in Appendix A.
3.0		ESSA Portfolio Management Team	• Made changes based on the Cybersecurity Information Sharing Act of 2015 Made changes in support of Automated Information Sharing (AIS) including adding Further Sharing and adding additional values
3.0a	June 27, 2019	DHS CISA/CSD	Updated CISAUSES on page 25 from: "The cybersecurity purposes allowed in the Cybersecurity Information Sharing Act of 2015 (Reference 36)." To: "Indicates that the CTI must be granted the protections spelled out in the Cybersecurity Information Sharing Act of 2015 (Reference 36), including that the government will only use the information for the cybersecurity purposes spelled out in that document."

ii The organizations that participated in the development of this ISA Access Control Specification were:

Federal Cybersecurity Centers
US Cyber Command (USCYBERCOM) Joint Operations Center (JOC)
Defense Cyber Crime Center (DC3)
National Cyber Investigative Joint Task Force (NCIJTF)
Intelligence Community Security Coordination Center (IC-SCC)
National Security Agency/Central Security Service (NSA/CSS) Threat Operations Center (NTOC)
Department of Homeland Security (DHS), National Cybersecurity and Communications Integration Center (NCCIC)

Approved by: _____ Date: 1 July 2019

Toni Benson Haynes
Section Chief, Cyber Threat & Risk Analysis
Cybersecurity Division
Cybersecurity and Infrastructure Security Agency

This page intentionally left blank.

Executive Summary

The vision for the Information Sharing Architecture (ISA) in support of the Enhance Shared Situational Awareness (ESSA) initiative is to create real-time cyber shared situational awareness based on machineto-machine information sharing as described by the ISA Shared Situational Awareness (SSA) Requirements. This cyber shared situational awareness supports both individual and integrated response actions to prevent malicious cyber activity and, when that fails, to protect and recover quickly from malicious cyber actions. At the core of that vision is automated, machine-to-machine information sharing across the cybersecurity community. The foundational work done by ESSA to establish a Federal Cybersecurity Information Sharing Community and the ISA provides an existing capability to support the requirements outlined in the Cybersecurity Information Sharing Act of 2015.

Information sharing across a Federal Cybersecurity Information Sharing Community requires a capability to protect and allow access to information in accordance with applicable information sharing agreements, policies, and laws. Capabilities must be put in place to ensure that information is only shared with those that should be allowed to see it, as determined by the information owner. As the quantity of shared information, the number of information types, and the number of participants' increase, the means of enforcing policies on information sharing and controlling access must be automated and scalable to meet mission needs. The Federal Cybersecurity Centers and Stakeholders in the ISA collaborated on a single, flexible approach to machine-based access control that builds upon advancements made by individual communities (e.g. Intelligence Community, Defense, Law Enforcement, etc.) and expands to meet the needs of the broad, cross-organizational cybersecurity community.

This Access Control Specification (ACS) document, the result of that collaboration, specifies the data elements required to implement automated access control systems based on the relevant policies governing sharing between participants. Initially developed to support information sharing by the Enhance Shared Situational Awareness (ESSA) initiative across the Federal Cyber Centers, the ACS specifies a common set of elements for tagging information and related common attributes that indicate characteristics of a person or system that allow automated decisions to be made regarding information

sharing. The ACS provides a structure to support expansion of the ESSA Community to include all Federal Entities in support of the Cybersecurity Information Sharing Act of 2015.

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

1 Introduction

This Information Sharing Architecture (ISA) Access Control Specification (ACS) document specifies the data elements required to implement access control mechanisms for exchanging cyber information across the community that has adopted the specification. The ACS is prescribed for Federal Entities that have signed the Enhance Shared Situational Awareness (ESSA) Multilateral Information Sharing Agreement, referred to as the ESSA Community. As the requirements of the Cybersecurity Information Sharing Act of 2015 are implemented, the ESSA Community will expand with additional signatories to the MISA to include additional Federal Entities. Because the ESSA Information Sharing Participants operate within all three classification domains (Top Secret, Secret, and Unclassified), the resource markings (data tags) and entity attributes are specified on all three domains in order to facilitate cross domain use of the information. Using a common set of resource markings and entity attributes and a common approach to access control enables integration and potential software reuse in different organizations.

This ISA ACS specifies resource markings and user entity attributes to support a collection of activities that include an initial access decision and also includes the necessary controls to inform subsequent or derivative activities, such as usage and further dissemination restrictions. Figure 1 illustrates the basic steps in making the initial access control decisions based on access rules that reside at each ESSA Information Sharing Participant (or their parent organization if the ESSA Information Sharing Participant is using their organization's enterprise services).

- *Authentication* – The process of verifying with a trusted identity provider the identity claimed by or assumed of an entity, such as a user, process, or device (i.e., check that I am who I say I am)
- *Authorization* – The process of verifying the access privileges granted to an authenticated user, program, or process, or the act of granting those privileges (i.e., check what I am allowed to see)

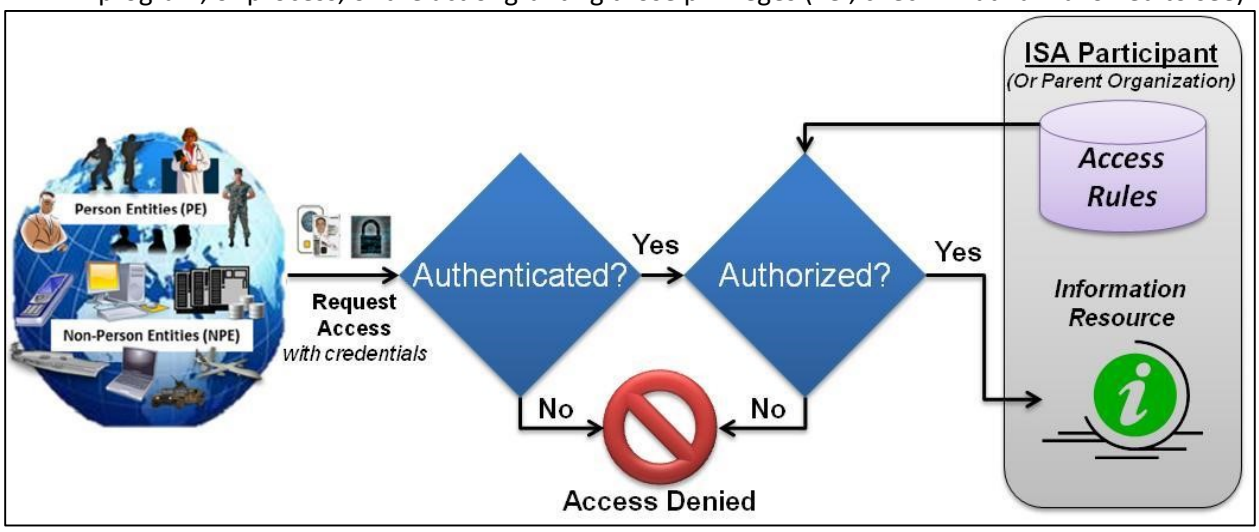

Figure 1: Overview of Access Control

Attribute-Based Access Control (ABAC) was selected by the ESSA Information Sharing Participants as the most appropriate approach to ISA authorization. ABAC is based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. Because the ISA operates across a

federation of organizations within the Federal government, there is no central authority to define roles, policies, or threat levels required for other approaches to authorization such as Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), or Risk Adaptable Access Control (RAdAC).

ABAC provides the resource owners the most flexible level of control for making access decisions. Under ABAC, access control policies can be created and managed without direct reference to potentially numerous users and resources, and users and resources can be provisioned without reference to access control policy. NIST Special Publication 800-162 "Guide to Attribute Based Access Control (ABAC) Definition and Considerations" provides additional information on establishing ABAC. (Reference 1)

As shown in Figure 1, authentication is a pre-requisite for authorization. Authentication is outside the scope of this document. Assuming an implemented digital identity management system is in place and that authentication has occurred, there are three major components that enable the authorization component of ISA access control (i.e. ABAC):

- Resource Attributes (often called data tags) assigned to information resources
- Entity attributes assigned to people (or machines/non-person-entities) describing their individual privileges with regard to information access
- Policies (or rules) that marry up the above two items

A common example of these components is classification/security clearance. A data resource has a classification. A person has a security clearance. The policy is that the person must have the same clearance level (or higher) as the classification of the data in order to see it. If there were only this one attribute of access control then the system would determine the data resource's classification and the individual's security clearance then apply the policy to determine if access is permitted. In cyber information exchange, there are a greater number of attributes of both data resources and people and more complex access rules that must be addressed.

Existing Policies as documented in sharing agreements, laws, Executive Orders, and other documents, specify the restrictions that ESSA Information Producers place on their data. These Policies include Executive Orders such as EO12333 and EO13556, the Multilateral Information Sharing Agreement (MISA), and others. The intent of the Access Control Specification (ACS) is to outline a set of resource and entity attributes that will allow ESSA Information Sharing Participants to tag data and entities so that, across the ISA, the sharing and usage restrictions identified in governing Policies can be communicated and enforced in an automated fashion. This document defines the access control attributes for people (or non-person-entities like machines and applications) and the attributes for data elements or resources.

1.1 ISA Background

The Enhance Shared Situational Awareness (ESSA) initiative and the Information Sharing Architecture (ISA) originated with National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23) that established a Comprehensive National Cybersecurity Initiative (CNCI). Of the 12 key cyber initiatives executed under CNCI, CNCI-5 directed the development of enhanced Shared Situational Awareness (SSA) of the US cyber domain, supporting real time information sharing for integrated operational action to improve the security of US Government assets and protect its critical infrastructure. At the end of FY13, some elements of the CNCI were sunset and others transitioned as their core mission continued forward and evolved. The core mission of CNCI-5, to

enhance shared situational awareness, continued forward and has evolved to enable integrated operational action under the name of Enhance Shared Situational Awareness (ESSA). To facilitate this continuous and evolving mission, the ESSA Portfolio Management Team (PMT), co-led by DHS, FBI, and NSA, was tasked by the staff of the National Security Council (NSC) to work with the Federal Cybersecurity Centers and other key stakeholders to implement the Information Sharing Architecture (ISA).

The foundational work done by ESSA to establish a Federal Cybersecurity Information Sharing Community and the Information Sharing Architecture (ISA) provides an existing capability to support the requirements outlined in the Cybersecurity Information Sharing Act of 2015.

This document, the ISA Access Control Specification, is an element of the following collection of ISA products:

- **ISA Framework** (Reference 2) – Defined the original ISA Framework, which provides the common taxonomy and understanding of ISA Functions and Enduring Functional Exchanges (EFEs) among cybersecurity partners and stakeholders
- **ISA Shared Situational Awareness (SSA) Requirements Document** (Reference 3) – Translates the ISA framework into a set of enterprise requirements and community standards and includes the maintained version of ISA Functions and EFEs ○ **ISA Access Control Specification (ACS)** – A supplement to the ISA SSA Requirements Document that provides a common specification to inform automated access control decisions at all classification levels
- **ISA Technical Implementation Plan** (Reference 4) – Describes how and when the capabilities defined in the ISA SSA Requirements Document will be built. The plan defines an incremental approach to ensure early mission benefit and support out-year flexibility

The ISA is not an end in and of itself. Each ESSA Information Sharing Participant agrees on commonly provisioned standards and solutions and then implements, manages, and maintains the capabilities. An ***ESSA Information Sharing Participant*** is defined as an organization that performs any of the ISA Functions defined in the ISA Framework and has accepted that information sharing, as defined by the ISA, is a part of the organization's cybersecurity mission. The capabilities described in the ISA are dependent upon machine processing of information and machine-level assurance that all policies and controls are applied in a trusted manner.

1.2 Access Control Attributes

The ESSA Information Sharing Participants have agreed to use Attribute Based Access Control (ABAC) to:

1. Ensure that information is only shared with those allowed to access it
2. Allow access control decisions to be made by the owner of the information.

As the quantity of shared information increases, the mechanism of controlling access must be automated to be scalable. Attributes provide a consistent and automated approach to sharing the details about people, non-person entities (e.g., machine analytics), and information resources.

Figure 2 is a refinement of Figure 1 that shows how pre-scripted access rules are applied to entity and resource attributes to make informed, automated access control decisions.

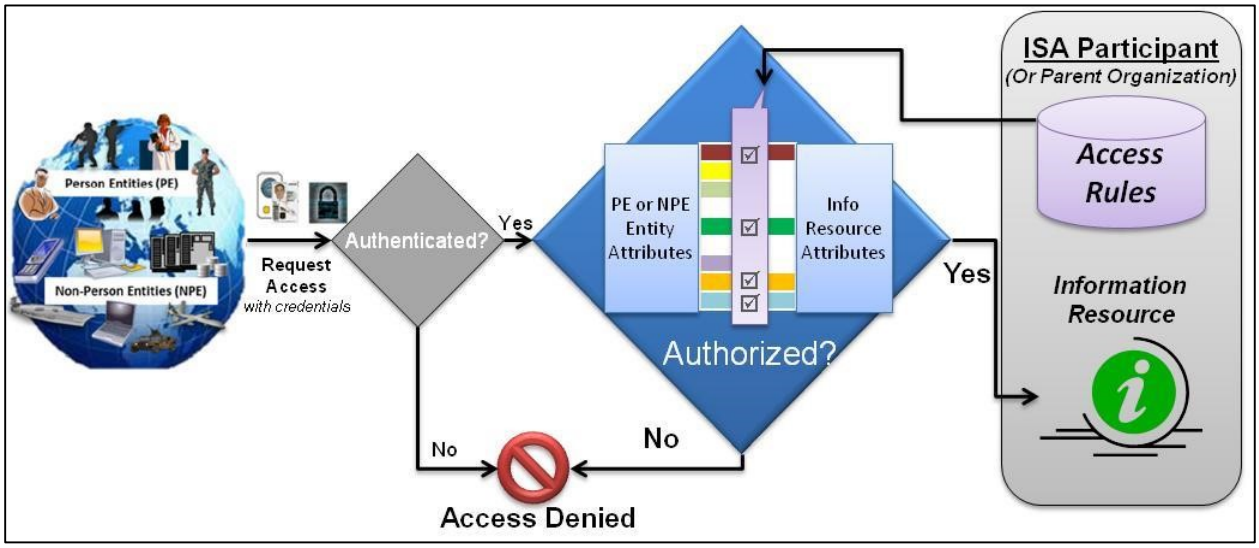

Figure 2: Use of Attributes in Authorization Component of Access Control

Automated access control depends on standardized attribute names and values among ESSA Information Sharing Participants. This document defines two types of attributes:

- *ISA Resource Attributes* – Characteristics of the resource being requested (e.g., classification of data). Resources include data, applications, and services.
- *ISA Entity Attributes* – Characteristics about the person or non-person entity (NPE) requesting access. These characteristics are used to make authorization decisions (e.g., clearance level).

The third major component of attribute based access control, the policies or rules, will be defined by the ESSA Information Sharing Participants. The ISA ACS provides the tools to express these policies consistently; however the policies are not comprehensively defined in this document. The intended relationships between the resource markings and the entity attributes are outlined in Section 4. Appendix E also includes an example access control rule set that may serve as a starting point for policy application. However, different ABAC implementations will dictate the specific language required to encode the policies.

Access control decisions can be logged to support subsequent auditing processes. For example, if remediation steps must be taken in the case of an unauthorized release, the logged access control decision and associated attributes assist with the remediation process.

1.3 Relationship to Other Access Control Efforts

This ISA ACS was developed by aligning and building upon existing efforts to minimize impacts on implemented, mature solutions while expanding to meet the needs of the cybersecurity community. The development of the ISA ACS leveraged the following:

- **Enterprise Data Header (EDH)** ○ **EDH Abstract Data Definition (ADD)** (Reference 12) - Defines at an abstract level the minimum set of data elements that could apply generically to any type of data in order to meet enterprise data management requirements.

  - **Smart Data EDH Data Encoding Specification (DES)** (Reference 14) – Specifies encoding guidance for the common set of fields defined in the EDH ADD.
- **Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance** (Reference 5) – Provides common segment architecture and implementation guidance for use by federal agencies as they continue to invest in ICAM programs.
- **IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS)** (Reference 6) – Governs the set of Intelligence Community (IC) enterprise identity attributes and associated values that must be supported by an Attribute Service participating in the IC's Unified Authorization and Attribute Service (UAAS) capability.
- **DoD Enterprise Identity Attribute Service (EIAS)** (Reference 7) – Provides Department of Defense (DoD) affiliation data on person and personnel-based attributes for authentication and authorization.
- **Department of Justice Global Federated Identity and Privilege Management (GFIPM)** (Reference 8) – Defines common syntax and semantics for metadata based on a well-grounded knowledge of the needs of real-world law enforcement information sharing systems.
- **Intelligence Community Enterprise Data Header (IC-EDH)** (Reference 9) – Defines a structured, verifiable representation of security metadata bound to intelligence data.

1.4 Scope of Document

This document establishes the specification for common ISA Resource Attributes (i.e. data tags) and ISA Entity Attributes for the purpose of access control within the ESSA Community, defined as those Federal Entities that have signed the ESSA Multilateral Information Sharing Agreement (MISA). It also includes resource attributes related to resource management and usage and dissemination restrictions. The scope of information resources being shared is defined by the ISA Enduring Functional Exchanges (EFEs) in the *ISA SSA Requirements Document* (Reference 3). The information resources include data elements that can be represented in the Structured Threat Information eXchange (STIX)™ format. STIX is becoming well-used in the cyber community. The ISA STIX Profile Description (Reference 21) provides additional information on the use of the resource markings specified in this Access Control Specification (ACS) for STIX documents.

The intended audience for this document is an organizational entity implementing access control solutions where there is an expectation of sharing information with or accessing information from other ESSA Information Sharing Participants. This document does not prescribe all access control attributes that an organization may need internal to their enterprise systems or within a community other than the ESSA Information Sharing Participants; the focus is on access control for cyber information shared outside of an organization.

This document expands upon access control requirements in the ISA SSA Requirements Document (Reference 3). While this document does not add new requirements, it provides derived requirements that give details on how to meet the parent ISA SSA Requirements. Derived requirements are included in tables with the parent requirement throughout the document and summarized in Appendix B: Summary of Derived ISA Requirements.

1.5 Definitions and Use of Terms

1.5.1 Entities

Entities are persons or non-person systems and are referred to as person entities and non-person entities (NPEs) in this ACS.

1.5.2 Entity Attributes

Entity attributes describe characteristics about a person or non-person entity (NPE).

1.5.3 Policies and policy rules

Policies, as a broad term of reference, are those documents that outline the general principles and acceptable procedures of a governmental organization. The ESSA Information Sharing Participants are governed by a large set of policies and the ACS will distinguish this high level Policy by capitalizing references. Many of these Policies relate to and specify restrictions regarding the access to, and sharing and handling of resources and data. Examples of high level Policies include EO12333, the Privacy Act, and the Multilateral Information Sharing Agreement.

Specific restrictions or requirements contained within these Policies may also be referred to as policies. The ACS will refer to these specific restrictions and requirements as “policies” with a small “p”. Of particular importance within the ACS are policies that govern the specific restrictions related to the management and control of resources. For example, the Department of Defense Policy governing control of classified information, DoD Manual 5200.01, details the specific policy that a person must have a clearance of Secret or higher in order to access Secret information.

Within access control systems, and in accordance with FICAM, policies are the rules and relationships between an entity requiring access and the resource that is being requested. When these policies are encoded, the ACS will use the term “policy rules” to differentiate these encoded statements from high level Policies and their specific restrictions and requirements (policies).

1.5.4 Resource

A resource is any data, information, document, application, analytic or service to be shared to requires tagging in order to allow controlled access.

1.6 Attribute Dependencies

The Resource Markings and Entity Attributes in this ACS have dependencies on additional technical specifications or additional documentation listed in Table 1-1. These dependencies may be related to the structure or values for the attributes. Table 1-1 is provided as a consolidated reference for those dependencies.

Table 1-1: Attribute Dependencies

Name	Description	Dependency

Smart Data Enterprise Data Header Implementation Profile for the Cyber Community (Reference 15)	The SD-EDH Cyber Profile provides the encoding modification and extensions in order to implement this ACS.	The versioning of the ACS and the Cyber Profile are maintained in alignment.
Enterprise Data Header Abstract Data Definition (ADD) (Reference 12) and Data Encoding Specification(DES) (Reference 13)	The ADD and DES provide the higher level definition and specification on which this ACS is based.	ACS v3.0 is aligned with EDH ADD Version 1.0 and DES Version 2.0
NSA Master Data Registry	Values for some of the Control Set resource attributes (SCI, LAC) in this ACS are dependent upon the Master Data Registry.	The Master Data Registry will serve as the authoritative source for the specified values.
IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3 (Reference 6)	The Entity Attributes in this ACS are based on UIAS. In particular, Entity values are aligned.	There is no direct dependency. ACS Entity attributes and values are specified for use. However, as the UIAS is updated, modifications to the ACS to maintain alignment are recommended.
GENC Specification Version 1.0 (Reference 31)	The GENC Standard specifies a profile of ISO 3166, Codes for the representation of names of countries and their subdivisions, that conforms to US Policy.	ACS v3.0 specifies GENC Edition 1.0.
ISO8601 Date and Time Specification (Reference 34)	ISO 8601 describes an internationally accepted way to represent dates and times using numbers.	ACSv3.0 specifies ISO8601 extended format with time zone designator Z.
Controlled Vocabulary Enumeration for USAgency (Reference 29)	Used for Admin Org	ACs v3.0 specifies USAgency-CVEnum Feb 2015

2 ISA Resource Attributes

Resource attributes are characteristics about the resource being requested, where resources are data, applications, or services. These resource attributes are frequently called data tags. These ISA Resource Attributes can be expressed via the Smart Data – Enterprise Data Header (SD-EDH) Cyber Profile, which was produced specifically to address the identified core data tagging requirements of the ISA community (Reference 15).

This ACS document specifies those resource attributes that an organization uses to tag information or resources shared with other ESSA Information Sharing Participants. As stated before, many organizations require additional attributes to meet other community or their own internal enterprise needs. For example, the IC commonly uses additional attributes beyond those listed here, but the addition of those attributes restricts those resources to the IC. Using additional access control resource attributes indicates that the resource is not a shared ISA information resource. If a participating organization wants to have a particular attribute associated with their shared ISA information, that attribute must be listed in this document or upon establishment of a registry, the attribute must be listed in the appropriate registry. This restriction promotes interoperability and facilitates integration. The ESSA Community created the Smart Data - Enterprise Data Header (SD-EDH) Cyber profile schema to facilitate applying ACS specified resource attributes to a resource. In addition, two Structured Threat Information eXchange (STIX) marking extension schemas were created to apply the markings to STIX documents. Additional information on the schemas is available on the ESSA Max.gov site (Reference 22).

TR-18	*"All data objects exposed for sharing shall have the Information Control metadata listed in Table 12: Summary of ISA Resource Attributes. " (Reference 3)*
TR-18.1	Upon sharing via ISA capabilities, ISA data producers shall limit access control resource attributes to those listed in the ISA ACS.
TR-18.2	ISA access control mechanisms shall make access control decisions using only ISA Resource Attributes

Note that several of the ESSA Information Sharing Participants store their information in a tagged fashion, using similar/identical resource tags to those found in this document. Others store their information in repositories and tag on data transfer. This document specifies how information is tagged when transferred or shared, and the format for internal storage of information is at the discretion of each participant. While the ACS requires data be tagged, the ACS does not specify a particular resource attribute management capability that an ESSA Information Sharing Participant must use to establish and bind attributes to resources.

TR-31	*"The access control business rules shall protect each ISA Participant's shared resources to the degree required by that Participant's information control tags." (Reference 3)*
TR-31.1	ISA information consumers shall maintain the data producer's access control constraints.

The types of ISA Resource Attributes are shown in Figure 3.

Resource Identifier
- A single unique identifier associated with the data

Resource Creation Time
- The creation date and time of the resource Date and

Responsible
- The information owner responsible for the resource

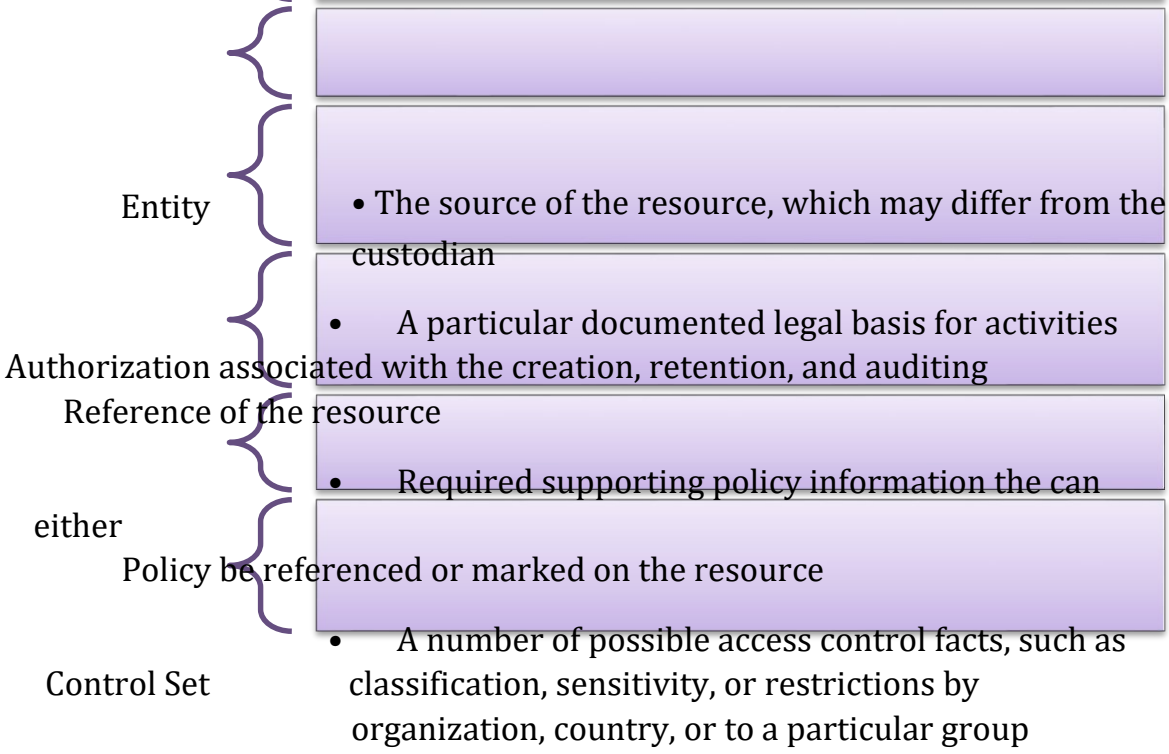

Figure 3: Organization of Resource Attributes

Table 2-1 summarizes the ISA ACS Resource Attributes, an indicator of whether the attribute is used in access control decisions, how policy rules are intended to be applied to the attribute, the multiplicity and allowable values, and an indicator as to whether the attribute (or its components) is required, as needed, or Not Applicable (N/A) at each network classification level.

Access Control decisions will be based on the specific attributes within the Control Set. Access control policy rules should be applied logically as AND across the set of all control set attributes. If a Control Set attribute is included, an entity requiring access to the data must have a corresponding attribute. The exceptions to this rule are the FD and CVT attributes which are not used in access control decisions. They remain in the control set to align with the Smart Data Enterprise Data Header (SD-EDH) Data Encoding Specification (Reference 13).

The Policy Rule Application column in the table describes the logic in the event that more than one value exists for a specific control set attribute. For example if the resource is marked with a Sensitivity of TEI and a Sensitivity of LES, an entity requesting access must have attributes corresponding to both sensitivities as indicated by an "AND" in the Policy Application column. If more than one Country restriction attribute is included (e.g. CTRY:USA CTRY:GBR) then an entity requesting access must have one or the other corresponding attributes, as indicated by an "OR" in the Policy Rule Application column. Additional examples are included in the Use Cases in Section 5.

Throughout this document, references are made to the multiplicity of attributes and parameters. Multiplicity defines the allowed number of occurrences of an attribute, and whether the attribute is required or optional. The following definitions are used to indicate whether specific attributes are required for resources on the three network fabrics:

- *Required* – This attribute must be provided for all data shared with ESSA Information Sharing Participants

- *As Needed* – This attribute is only supplied, at the discretion of the data producer, if it is applicable to the resource. The consumer shall be able to handle the attribute appropriately if present and respond gracefully if not present.
- *N/A* – The attribute is not valid for the indicated network classification level and should not be included.

Table 2-1: Summary of ISA Resource Attributes

ACS Resource Attribute Name	May be Used in Access Control Decision	Policy Rule Application	Multiplicity	Allowable Values	Network		
					Top Secret	Secret	Unclassified
ResourceAccountingGroup							
Identifier	No		Min=1, Max=1	Example: isa:guide.19001.40af97be-00bf-4648-9e70-296a6a8edab2[1]	Required	Required	Required
CreateDateTime	No		Min=1, Max=1	Example: 2014-09-11T19:00:00.000Z	Required	Required	Required
ResponsibleEntity	No		Min=1, Max=1	Includes one CUST and may include one ORIG	Required	Required	Required
Custodian	No		Min=1, Max=1	Use allowable values from ORG	Required	Required	Required
Originator	No		Min=0, Max=1	Use allowable values from ORG	As needed	As needed	As needed
AuthRef	No		Min=0, Max=1	Example: urn:isa:authority: CFR2013_32_2_236	As needed	As needed	As needed

ACS Resource Attribute Name	May be Used in Access Control Decision	Policy Rule Application	Multiplicity	Allowable Values	Network		
					Top Secret	Secret	Unclassified
ControlPolicyGroup							

[1] The ISA has been assigned a GUIDE (Globally Unique Identifier for Everything) prefix of 19001 for production and 999191 for test use. CIA is the Executive Agent for GUIDE on behalf of the Intelligence Community.

AuthRef	No		Min=0, Max=1	Example: urn:isa:authority:CFR2013_32_2_236	As needed	As needed	As needed
PolicyRef	No		Min=1, Max =1	urn:isa:policy:acs:ns:v3.0?query components Query components are specified in Section 2.2.1. (Additional values for the policy reference are permitted as space separated urn.)[2]	Required	Required	Required
Policy	No		Min=0	May include one or more of: Original Classification, Derivative Classification, Declassification, Resource Disposition, Public Release, Access Privilege, or Further Sharing	As needed	As needed	As needed
Original Classification[3]	No		Min=0, Max=1	Subelements include: classifiedBy, classifiedOn, classificationReason, compilationReason	As needed	As needed	N/A
classifiedBY	No		Min=1, Max=1	Person identifier			
classifiedOn	No		Min=0, Max=1	YYYY-MM-DD			
classificationReason	No		Min=0, Max=1	Narrative			
compilationReason	No		Min=0, Max=1	Narrative			
Derivative Classification	No		Min=0, Max=1	Subelements include: classifiedBy, classifiedOn, derivedFrom	As needed	As needed	N/A
classifiedBY	No		Min=1, Max=1	Person identifier			
classifiedOn	No		Min=0, Max=1	YYYY-MM-DD			

	May be		Multiplicity	Allowable Values	Network

[2] Originators must ensure that Policy References do not provide conflicting policy.

[3] For classified documents, either an OriginalClassification or DerivativeClassification Authority is required.

ACS Resource Attribute Name	Used in Access Control Decision	Policy Rule Application			Top Secret	Secret	Unclassified
derivedFrom	No		Min=1, Max=1	Narrative			
Declassification	No		Min=0, Max=1	Subelements include: declassExemption, declassPeriod, declassDate	As needed	As needed	N/A
declassExemption	No		Min=0, Max=1	Exemption codes (EO13526)			
declassPeriod	No		Min=0, Max=1	Time in years from a create date when a resource will be declassified			
declassDate	No		Min=0, Max=1	YYYY-MM--DD			
declassEvent	No		Min=0, Max=1	Narrative			
ResourceDisposition	No		Min=0, Max=1	Subelements include: dispositionProcess, dispositionDate	As needed	As needed	As needed
dispositionProcess	No		Min=1, Max=1	DSTRCT, TRNSFR[4]			
dispositionDate	No		Min=1, Max=1	YYYY-MM--DD			
PublicRelease	No		Min=0, Max=1	Subelements include: releasedBy, releasedOn	As needed	As needed	As needed
releasedBy	No		Min=1, Max=1	Narrative			
releasedOn	No		Min=0, Max=1	YYYY-MM-DD			

[4] Disposition of Federal Records: A Record's Management Handbook 2000 Web Edition <http://www.archives.gov/records-mgmt/publications/disposition-of-federalrecords/chapter-4.html#DispInstructions>
DoDDirective 5015.2, "DoD Records Management Program," March 6, 2000

AccessPrivilege	No		Min=0	Subelements include: PrivilegeAction, PrivilegeScope, ruleEffect Default of “permit” or “deny” set for the Policy	As needed	As needed	As needed

ACS Resource Attribute Name	May be Used in Access Control Decision	Policy Rule Application	Multiplicity	Allowable Values	Network		
					Top Secret	Secret	Unclassified
PrivilegeAction	No		Min=1, Max=1	DSPLY, IDSRC, TENOT, NETDEF, INTEL, REQUEST, TEARLINE, OPACTION, LEGAL, ANONYMOUSACCESS, CISAUSES, ALL	As needed	As needed	As needed
PrivilegeScope	No		Min=1	The privilegeAction will apply to all organizations include in the privilegeScope. Allowed fields include: • Country (CTRY) • Organization (ORG) • Entity (ENTITY) • SHAR • ALL	As needed	As needed	As needed
ruleEffect	No		Min=1; Max=1	permit or deny	As needed	As needed	As needed
FurtherSharing	No		Min=0	Subelements include:sharingScope and ruleEffect Default of “permit” or “deny” set for the Policy	As needed	As needed	As needed
sharingScope	No		Min=1;Max=1	The sharingScope values may include ORG values, FOREIGNGOV or SECTOR	As needed	As needed	As needed
ruleEffect	No		Min=1; Max=1	permit or deny	As needed	As needed	As needed
ControlSet	Yes		Min=1, Max=1	Paired tokens with the prefix and values below	Required	Required	Required

Classification (CLS)	Yes	Clearance must be higher than or equal to CLS	Min=1; Max=1	U, C, S, TS	Required	Required	Required
ACS Resource Attribute Name	**May be Used in Access Control Decision**	**Policy Rule Application**	**Multiplicity**	**Allowable Values**	**Network**		
					Top Secret	**Secret**	**Unclassified**
SCI Controls (SCI)	Yes	AND	Min=0	MDM SCI Control List	As needed	N/A	N/A
Logical Authority Category (LAC)	Yes	AND	Min=0	NSA Master Data Registry Logical Authority Categories	As needed	N/A	N/A
Formal Determination (FD)	No		Min=0	PUBREL, NF, AIS, PII-NECESSARY-TO-UNDERSTAND-THREAT, PII-NOT-PRESENT, FOUO	As needed	As needed	As needed
Caveat (CVT)	No		Min=0	FISA[5], POSSIBLEPII, CISAPROPRIETARY	As needed	As needed	As needed
Sensitivity (SENS)	Yes	AND	Min=0	NTOC_DHS_ECYBER_SVC_SHARE.NSA.NSA, PCII, LES, INT, PII, PR, TEI	As needed	As needed	As needed
Shareability (SHAR)	Yes	OR	Min=0	NCC, EM, LE, IC	As needed	As needed	As needed
Country (CTRY)	Yes	OR	Min=0	GENC Specification	As needed	As needed	As needed
Organization (ORG)	Yes	OR	Min=0	Appendix A	As needed	As needed	As needed
Entity (ENTITY)	Yes	OR	Min=0	MIL, GOV, CTR, SVR, SVC, DEV, NET[6]	As needed	As needed	As needed

[5] Based on DoD Information Security Manual, (Reference 17).

[6] Based on Unified Identity Attribute Set (Reference 6).

2.1 Resource Accounting Group

The Resource Accounting Group groups those resource attributes that are necessary for sourcing, tracking and auditing. The elements in the Resource Accounting Group will be used minimally at the resource root level and may be used at the resource component level when resource accounting attributes need to be reset. Each attribute section includes a table that indicates the requirement for the attribute at the root level.

2.1.1 Resource Identifier

This required element holds a single unique identifier associated with the resource. This value can be used for tracking data provenance, executing data retraction, and enforcing auditing requirements. The Resource Identifier will use a format that includes a prefix and an RFC4122 suffix. The prefix used will include the ISA common prefix (GUIDE prefix). The ISA has been assigned a GUIDE[7] (Globally Unique Identifier for Everything) prefix of 19001 for production and 999191 for test use. It is recommended that RFC 4122 Version 4 UUIDs be used for the suffix; however, other versions are permitted.

TR-18.3	Data producers shall provide a unique resource identifier for each shared resource.

Name: Identifier urn:isa:acs:ns:v3.0:identifier	**TS** [8]	**S**	**U**
Definition: Attribute to hold the identifier of the data object.	Required	Required	Required
Multiplicity: Single instance permitted.			
Format: xsd:QName (will include a uri of isa: followed by a suffix of format xsd:NCName) Examples: isa:guide.19001.Observable-40af97be-00bf-4648-9e70-296a6a8edaa4 isa:guide.19001.40af97be-00bf-4648-9e70-296a6a8edab2 isa:guide.999191.Observable-40af97be-00bf-4648-9e70-296a6a8edaa4			

2.1.2 Resource Creation Date and Time

This required element provides the creation date and time of the associated resource as identified by the Identifier. This value supports a number of functions including enforcing data retention policies and auditing requirements.

TR-18.4	Data producers shall provide a resource creation date and time for each shared resource.

[7] CIA, the Executive Agent for GUIDE on behalf of the Intelligence Community, provided these prefixes to ISA. [8] In each resource marking table, the TS, S and U refer to the network on which the resource resides, not the classification of the resource.

Name: CreateDateTime urn:isa:acs:ns:v3.0:createdatetime	**TS**	**S**	**U**
Definition: The created date and time of the associated resource.	Required	Required	Required
Multiplicity: Single instance permitted.			
Format: xsd:dateTime where Date and Time are using ISO8601 extended format with time zone designator Z as in the example. Example: 2006-05-04T18:13:51Z			

2.1.3 Responsible Entity

The Responsible Entity data field can be used by the data producer to indicate two types of responsible entities, a custodian and an originator, because they may not always be the same. For example, a data producer may desire to share information from a private organization, such as an internet service provider. In this case, the government organization may create the data tags to allow sharing across the ISA of the resource, but it is not the original source of the information.

Name: Responsible Entity urn:isa:acs:ns:v3.0:responsibleentity	**TS**	**S**	**U**
Definition: The responsible entity for the associated resource. This element allows for multiple tokens.	Required	Required	Required
Multiplicity: Single instance permitted.			
Format: xsd:NMTOKENS for custodian and originator as described below Example: CUST:USA.USAF.DC3 ORIG:COM.FIREEYE			

2.1.3.1 *Custodian*

This required sub-element represents the data producer that is responsible for providing the associated resource to be shared. It is represented as an organization token. This value is necessary for auditing and enforcing data retention and provenance policies.

TR-18.5	Data producers shall provide a custodian for each shared resource.

Name: Custodian (CUST)	**TS**	**S**	**U**
Definition: The custodian for the associated resource. This element uses organizational tokens. Note that if a custodian requires anonymity for further dissemination then a Privilege Action (Section 2.2.2.1) denying identification of the source should be used.	Required	Required	Required
Multiplicity: Single value permitted.			

Format: xsd:NMTOKENS with allowable values listed in Appendix A: List of Organizations. Example: CUST:USA.USAF.DC3

2.1.3.2 *Originator*

This optional sub-element represents the originating organization for the associated resource. If not present then the origin of the information is unspecified. It is represented as an organization token. It is recommended that the organizations in Appendix A be used. However, additional tokens may be created to specify the originator.

Certain Originators may require anonymity to protect their identity. This is common when dealing with a cybersecurity threat or incident where the originator is an entity in the Private Sector. Cover terms (e.g., USENERGY01) assigned to an entity should be carried through anytime the resource is shared or a Privilege Action (Section 2.2.2.1) denying identification of the source should be used.

Name: Originator (ORIG)	**TS**	**S**	**U**
Definition: Specifies the source of the resource, which may differ from the custodian. Note that if a source entity requires anonymity for further dissemination then a Privilege Action (Section 2.2.2.1) denying identification of the source should be used.	As Needed	As Needed	As Needed
Multiplicity: Single value permitted.			
Format: xsd:NMTOKENS of recommended values listed in Appendix A: List of Organizations. Example: ORIG:COM.FIREEYE would represent the commercial company FireEye.			

2.1.4 Authorization Reference

This optional element provides a means of indicating a particular documented legal basis for mission activities associated with the creation, retention, use, and auditing of the associated resource. Initially, the list of referenced authorizations will be provided as text files on the ESSA Max.gov site (Reference 22). In the long term, it is intended that a shared service be hosted by the ISA Shared Capability Provider for necessary policy and authorization references.

This field captures the legal authority under which the content was created, not the limitation on sharing the content. This field is used for auditing and records management, not for access control decisions. In some cases, the Authority Reference is needed by ESSA Participants to be included in the Control Policy Group as well as the Resource Accounting Group.

Name: Authorization Reference urn:isa:acs:ns:v3.0:authref	**TS**	**S**	**U**
Definition: A means of indicating a particular documented legal basis for mission activities associated with the creation, retention and use of a resource.	As Needed	As Needed	As Needed
Multiplicity: Single instance permitted.			

Format: URI Example: urn:isa:authority:CFR2013_32_2_236 Example Values: Values listed on Max.gov. https://community.max.gov/download/attachments/695866673/ISA%20AuthRef%20Table.txt?api=v2 There should normally be at most one reference to an authority but if multiple authorities are referenced, they are provided as multiple space delimited values of a single instance of AuthRef.

2.2 Control Policy Group

The Control Policy Group includes attributes necessary for the determination of allowable access as well as restrictions on usage and further sharing. All resources will include the Control Policy Group at the document level and may apply the Control Policy Group on a component level. The Authority Reference as described in Section 2.1.4 is allowed in both the Resource Accounting and Control Policy Groups. The SD-EDH construct allows for both the de-referencing of policy information or the inclusion of policy information on the resource as well as tagging of control information on the resource.

2.2.1 Policy Reference

The Policy Reference (PolicyRef) is used to provide a reference to policies related to the resource. Allowing policies by reference can reduce the amount of metadata that must be carried with data and provides flexibility to modify policies without requiring changes to existing marked resource. Initially, the list of referenced policies will be provided as text files on the ESSA Max.gov site (Reference 22). In the long term, it is intended that a shared service be hosted by the ISA Shared Capability Providers for necessary policy and authorization references.

At a minimum, ISA resources will include a reference to the ISA Access Control Specification (ACS)[8] at the document level. The ACS PolicyRef expressed as a urn will also include a query component field. There are two parts of the query component: *privdefault* that will indicate the Access Privilege default for all ACS-listed privilege actions (See Section 2.2.2.1) and *sharedefault* that will indicate the scope of further sharing that is permitted once an entity has been granted access (See Section 2.2.2.2). For a urn such as the PolicyRef, the query component represents some operation applied to the object. In this case, it is used to refer to the default value for all of the actions defined by Access Privilege and the sharing restrictions defined by Further Sharing.
A single PolicyRef element may be included in a marking structure but multiple values are permitted as space separated urn for the single PolicyRef element. If more than one reference is supplied, care must be taken by the originator that the policies specified do not conflict.

Name: Policy Reference urn:isa:acs:ns:v3.0:policyref	**TS**	**S**	**U**

[8] Although the ACS is not a encoded access control policy, the ACS is a technical "policy" document and is an appropriate reference in this section.

Definition: A means of indicating a particular documented policy related to the sharing of a resource.	Required (for ACS; others as needed)	Required (for ACS; others as needed)	Required (for ACS; others as needed)
Multiplicity: A single PolicyRef element may be included in a structure but multiple values are permitted as space separated urn.			
Format: URI One of the following values must be included: urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=deny urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=deny			

2.2.2 Policy

While the Policy Reference (previous section) is the preferred method of referencing policy information about a resource, there are certain situations where actual policy information is required to be embedded in the resource. For example, CAPCO policy specifies that classified data must be marked with a classification authority block that has changeable values based on the content of the resource. The values for the classification authority block are obtained from PolicyRule substitutions allowed in this Policy section. Note that the Policy section is not used directly to inform access control decisions. Those attributes necessary for access control are included in the Control Set.
The available substitution groups and their components are shown in Figure 4.

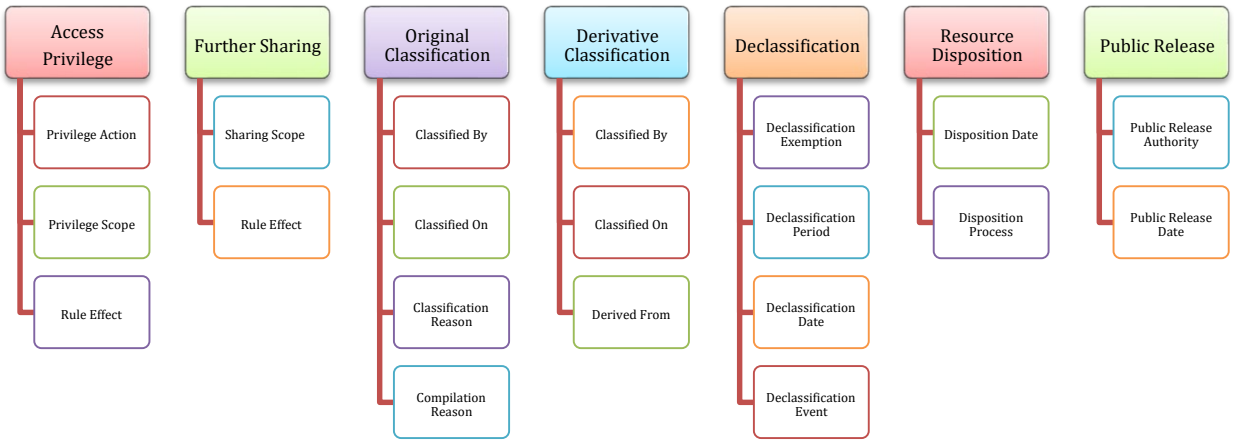

Figure 4: Substitution Groups for the Policy Attribute

2.2.2.1 *Access Privilege*

In order to support near-real time actions necessary to conduct cyber defense, for example automated population of intrusion protection systems, the ESSA Community requires a capability to specify or limit the actions that are allowed with a resource following an access decision. The Access Privilege element allows restriction on the actions that are permitted by an ESSA Information Sharing Participant following an access decision. Access Privilege may be employed on an as needed basis but if employed, only the allowable values below may be used. For every privilegeAction, a privilegeScope and ruleEffect are mandatory. Note that the default effect (permit or deny) on all actions is set with a query component of the PolicyRef to the ACS (Section 2.2.1).

Name: Access Privilege urn:isa:acs:ns:v3.0:accessPrivilege			**TS**	**S**	**U**
Definition: A means of limiting or permitting specific actions following access control decisions.			As needed	As needed	As needed
Multiplicity: Multiple instances are permitted. For each AccessPrivilege, a single privilegeAction is permitted. For each privilegeAction, a single ruleEffect and multiple PrivilegeScope are permitted.					
Element:	Multiplicity:	Format:	Allowable values:		
privilegeAction	Single value	xsd:NMTOKEN	DSPLY, IDSRC, TENOT, NETDEF, LEGAL, INTEL, TEARLINE, OPACTION, REQUEST, ANONYMOUSACCESS, CISAUSES, ALL		
privilegeScope	Multiple values	xsd:NMTOKENS	Same as ORG, CTRY, SHAR or ENTITY and additionally ALL		
ruleEffect	Single value	xsd:NMTOKEN	permit or deny		

The defined access privilege actions are based on the ISA Phase 1 document (for Network Defense and Operational Action) (Reference 2), the NSS Security Manual (to support Display Only) (Reference 17), and existing Policies that specify usage restrictions or permissions. These include:

- DSPLY: display – The action of displaying, either in a hard copy document or a visual presentation, the resource. See the Use Case below. DSPLY should be used to permit display when there is generally a global deny for all actions.
- IDSRC: identify source – The action of identifying the source of the resource further than the entity receiving the resource. When set to deny, attributes or elements in the resource that identify the source and custodian must be removed or replaced prior to additional actions being taken. This restriction applies not only to the elements in the header of the resource but may also apply to elements within the body of the document being shared. The use of IDSRC does not authorize any

changes to markings on the resource. For example, the removal of the source information will not change the classification of the resource.

- TENOT: targeted entity notification – The action of notifying a targeted entity of a cybersecurity incident based on the resource.
- NETDEF: computer network defense action – The action of taking network defense actions including detection and mitigation, remediation, and local analysis and signature development, based on the resource.
- LEGAL: legal proceedings – The action of using the resource in legal proceedings.
- INTEL: intelligence analysis – The action of conducting additional intelligence analysis based on the resource.
- TEARLINE: The action of removing and taking further action on components of a resource based on their component markings. To be tear-lineable indicates that marked components of a document may be removed and treated as individually marked components. When set to deny, even though there may be components with fewer restrictions than the overall document, they may not be removed.
- OPACTION: operational action – The action of conducting cyber-based operations applied to adversary capabilities based on the resource.
- REQUEST: accessPrivilege waiver request – The action of requesting a waiver to an accessPrivilege restriction. When set to deny, the originator will not consider specific requests to take actions based on the resource.
- ANONYMOUSACCESS: The action of allowing anonymous access to the resource. This action is included to support the restrictions placed on the indicators shared with the US government from the DHS Automated Indicator Sharing (AIS) program.
- CISAUSES: Indicates that the CTI must be granted the protections spelled out in the Cybersecurity Information Sharing Act of 2015 (Reference 36), including that the government will only use the information for the cybersecurity purposes spelled out in that document.

To support a Display Only Use Case, the PolicyRef level default would be set to **deny**, privilegeAction would include **DSPLY**; privilegeScope would include **ORG:ALL**; ruleEffect would be set to **permit**.

To allow actions with non-attribution, the PolicyRef level rule would be set to **permit**, privilegeAction would include **IDSRC**, privilegeScope would include **ORG:ALL**, ruleEffect would be set to **deny**. In such a case, all references to the source and custodian of the data must be replaced or removed. In the markings, the CUST must be replaced and AddlReference and ORIG must be removed by the data resource recipient prior to any further action regardless of additional markings. Additional references within the resource may also need to be removed.

To deny one specific further action that may be taken by one specific organization upon access to resource, the PolicyRef level rule would be set to **permit**, privilegeAction would include ***ACTION*** (one of the defined), privilegeScope would include ***ORG*** (one of the defined), and ruleEffect would be set to **deny**. For example <privilegeAction> TENOT, <privilegeScope> USA.FBI, <ruleEffect> deny would restrict FBI from conducting targeted entity notification.

In a broader case, to limit all organizations from conducting an action, the PolicyRef level rule would be set to **permit**, privilegeAction would include ***ACTION*** (one of the defined), privilegeScope would include **ORG:ALL**, and ruleEffect would be set to **deny**.

Additional use cases are included in Section 5.

2.2.2.2 *Further Sharing*

The Further Sharing element restricts the further sharing of a resource following an access decision. The Further Sharing element facilitates the appropriate handling of resources by ESSA Information Sharing Participants who have additional sharing agreements or relationships outside of the ESSA Community. Further Sharing will provide these Participants with the necessary information to determine if the resource can be further shared beyond the ESSA Community. Further Sharing may be employed on an as needed basis but if employed, only the allowable values below may be used. If used, the sharingScope and ruleEffect are mandatory. Note that the default effect (permit or deny) on all further sharing is set with a query component of the PolicyRef to the ACS (Section 2.2.1) similar to setting AccessPrivilege default.

Name: Further Sharing urn:isa:acs:ns:v3.0:furtherSharing			**TS**	**S**	**U**
Definition: A means of limiting or permitting further sharing following access control decisions.			As needed	As needed	As needed
Multiplicity: Multiple instances are permitted.					
Element:	Multiplicity:	Format:	Allowable values:		
sharingScope	Multiple values	xsd:NMTOKENS	Same as ORG and additionally FOREIGNGOV, SECTOR		
ruleEffect	Single value	xsd:NMTOKEN	permit or deny		

The defined further sharing scopes are based on the need to support policies in support of the Automated Indicator Sharing (AIS) program implemented in conformance with Executive Order (EO) 13691. (Reference 30) A sharingScope of FOREIGNGOV indicates to a resource consumer that the resource may be further shared with foreign governments under the authorities of the consumer. A sharingScope of SECTOR indicates to a resource consumer that the resource may only be shared with the sector for which the consumer is the Sector Specific Agency as defined in Presidential Policy Directive-21. (Reference 35)

2.2.2.3 *Original Classification*

This data tag provides details for generating a classification authority block for presentation of a classified resource to an operator. Either the Original Classification or the Derivative Classification is required for classified resources, as appropriate. Details regarding the basic encoding specification detail for Original Classification are included in the Smart Data – Enterprise Data Header (EDH) Implementation

Profile for the Cyber Community (Reference 15). The following sub-fields are used to capture the details for original classification:

- *Classified By*: The person with the original classification authority who made a classification determination.
- *Classified On*: The date an original classification determination was made.
- *Classification Reason*: The rationale for an original classification determination.
- *Compilation Reason*: The rationale for assigning a higher classification level than a simple roll-up of its portions would indicate.

2.2.2.4 *Derivative Classification*

This data tag provides details for generating a classification authority block for presentation of a classified resource to an operator. Either the Original Classification or the Derivative Classification is required for classified resources, as appropriate. Details regarding the basic encoding specification detail for Derivative Classification are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community (Reference 15). The following sub-fields are used to capture the details for derivative classification:

- *Classified By*: The person with the original classification authority who made a classification determination.
- *Classified On*: The date an original classification determination was made.
- *Derived From*: A citation of the original classification guidance used for a derivative classification.

2.2.2.5 *Declassification*

This data tag provides the declassification instructions associated with an original or derived classification for generating a classification authority block for presentation of a classified resource to an operator. Details regarding the basic encoding specification detail for Declassification are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community (Reference 15). The following sub-fields are used to capture the details for declassification:

- *Declassification Exemption*: A basis for a resource not being subject to standard automatic declassification processes.
- *Declassification Period*: A duration of time in years for calculating from a create date or classification date when a resource will be automatically declassified if not exempt.
- *Declassification Date*: A date upon which a resource will be automatically declassified if not exempt.
- *Declassification Event*: A future occurrence upon which a resource will be automatically declassified if not exempt.

2.2.2.6 *Resource Disposition*

This optional element can be used to provide a fixed date and time at which an action is to be taken on the associated resource, such as destruction. Retention can be enforced through the use of this element or through the use of policies. This attribute allows for honoring ad hoc (i.e., not policy based) retention limitation requests from information creators such as private industry. Details regarding the basic encoding specification detail for Resource Disposition are included in the Smart Data – Enterprise Data

Header (EDH) Implementation Profile for the Cyber Community (Reference 15). The following sub-fields are used to capture the details for resource disposition:

- *Disposition Date*: The time that the declared disposition process type is to be initiated.
- *Disposition Process*: The allowed disposition process to be performed (e.g., destruction).

2.2.2.7 *Public Release*

This element will be used to provide the release authority and date for resources that have been through a formal public release determination process. Resources will further be marked with a formal determination marking (FD=PUBREL) (See Section 2.2.3.4). Details regarding the basic encoding specification detail for Public Release are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community (Reference 15). The following sub-fields are used to capture the details for public release:

- *Released By*: The authority that authorized the public release.
- *Released On*: The date of public release.
- Values used to indicate the release authority (releasedBy) will be established by the ESSA Information Sharing Participants and should identify authorities, not individuals.

2.2.3 Control Set

The Control Set is the group of data tags that are used to inform automated access control decisions as represented in Figure 5.

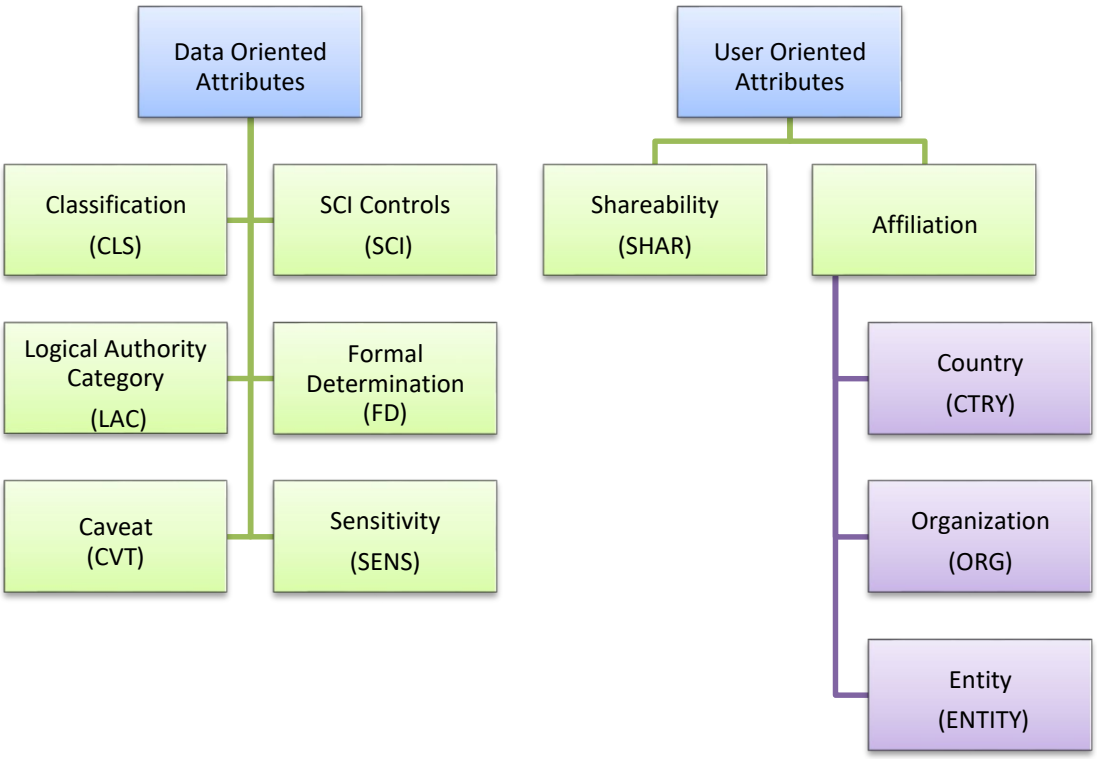

Figure 5: Data-Oriented and User-Oriented Attributes in the Control Set

Data-Oriented Attributes characterize the sensitivity of the data. If any of these controls are used then an entity would be required to meet every single sensitivity criterion in order to access the resource. This may be characterized as a Boolean "And" both within each attribute and across them. For example, if a resource is Top Secret, requires two different SCI restrictions, and has a particular Sensitivity, then to gain access to that resource the entity must have a TS clearance, must have both SCI accesses, and also must be a member of the Access Group that is permitted to access data of that Sensitivity.

User-Oriented Attributes characterize the group of people or entities that should be able to access the data. If multiple values are listed for an attribute, then the entity would need to be able to satisfy one of the restrictions. This may be characterized as a Boolean "Or" within each attribute and an "And" across them. For example, if the data is limited to citizens of two possible countries and tagged with three Shareability attributes, then to gain access the entity must be a citizen of one of those two countries and is in at least one of the Access Groups.

The implementation of the Control Set using the SD-EDH Cyber Profile uses tokens to express the subelements of the Control Set. For example, the classification of an unclassified resource is represented as CLS:U. The entire control set is a set of tokens. Access Control policy rules are applied across the set of control set tokens.
Much of the structure of the Control Set is based on requirements related to support for Executive Order 13526, Classified National Security Information (Reference 23). Where possible, alignment with the Information Security Manual (ISM) (Reference 17) marking system and its implementation in Intelligence Community Technical Specifications was maintained. Appendix D: Deltas between ISA ACS Resource Attributes and IC Security Marking Encodings details some of the differences and justifications for changes in order to support ISA requirements.

2.2.3.1 *Classification*

The Classification token contains the classification of the data based on the Executive Order 13526, Classified National Security Information (Reference 23) and the Information Security Manual (ISM) (Reference 17) marking system. Unclassified information will include a classification marking.

TR-18.6	Data producers shall provide the classification for each shared resource.
TR-83	*"The access control mechanism shall authenticate and authorize the consumer." (Reference 3)*
TR-83.1	The access control mechanism shall only grant access to consumers that hold an equivalent or higher clearance than the classification of the resource.

Name: Classification (CLS)	**TS**	**S**	**U**
Definition: The classification associated with the resource. For the ISA Cyber domain, the default is US marking systems.	Required	Required	Required
Multiplicity: Single classification token permitted.			

Format: Token of format CLS:value Allowable Values: TS, S, C, U

2.2.3.2 *Sensitive Compartmented Information Control System*

This element is used to capture that the resource contains Sensitive Compartmented Information (SCI), classified national intelligence information concerning or derived from intelligence sources, methods, or analytical processes which is required to be handled within formal access control systems established by the Director of National Intelligence (DNI). (Reference 17) This element is only used on the TS fabric.

Because this attribute is characterizing the sensitivity of the data, an entity must meet all of the restrictions defined in this attribute in order to gain access.

TR-83.2	If a resource has special control restrictions, then the access control mechanism shall only grant access to consumers that hold all of the corresponding special control permissions.

Name: SCI Controls (SCI)	**TS**	**S**	**U**
Definition: Indicators identifying sensitive compartmented information control system(s). This attribute requires that an entity (person or nonperson) be granted specific permission to access or process resources covered by SCI Control Systems and Compartments.	As Needed	N/A	N/A
Multiplicity: Multiple values permitted.			
Format: Token of format SCI:value Allowable Values: As listed in NSA's Master Data Registry			

2.2.3.3 *Logical Authority Category*

The Logical Authority Category represents classes of authority upon which data can be generated or acquired and that can be used to apply mandatory special access control and handling policies. This resource marking covers a class of mission activity authorizations that is based on common characteristics such as legal basis, sponsor, granting authority, targets, specific authorized activities, and data handling rules and procedures. Logical Authority Categories are assigned to data resources on the TS fabric.

Because this attribute is characterizing the sensitivity of the data, an entity must meet all of the LAC restrictions associated with the resource to gain access.

TR-83.8	If a resource has LAC restrictions, then the access control mechanism shall only grant access to consumers that hold all of the corresponding LAC permissions.

Name: Logical Authority Category (LAC)	**TS**	**S**	**U**
Definition: Specifies the authorities related to the resource that must be held by an entity authorized to access and/or discover the resource.	As Needed	N/A	N/A
Multiplicity: Multiple values permitted.			

Format: Token of the format LAC:value Allowed Values: • Values listed for the Logical Authority Categories attribute from NSA's Master Data Registry

2.2.3.4 *Formal Determination*

The Formal Determination attribute is an indication that a formal process has been undertaken to make a determination about the resource, such as whether a resource has been approved for public release.

TR-18.8	If a resource has sensitivity or shareability restrictions, then Formal Determination shall not include Public Releaseable.

Name: Formal Determination (FD)	**TS**	**S**	**U**
Definition: Indicates other formal determinations beyond classification that have been applied to a resource.	As needed	As needed	As needed
Multiplicity: A single attribute instance with multiple values permitted.			
Format: Attribute with allowable Tokens Allowable Token Values: • PUBREL – Approved for Public Release • NF – NOFORN • AIS – Automated Indicator Sharing • PII-NECESSARY-TO-UNDERSTAND-THREAT • NO-PII-PRESENT • FOUO – For Official Use Only			

PUBREL: PUBREL is an indication that the resource has been through a formal process that has determined that the resource is releasable to the public. Resources that are approved for public release do not have access restrictions. This also implies that authentication is not necessary for access control purposes. Resources marked with a formal determination of PUBREL will also include a PublicRelease attribute that includes the release authority and date. (See Section 2.2.2.7) Classified resources will not be marked as publically releasable.

NOFORN, is specified in the DoD Information Security Manual (Reference 17) and further specified in Intelligence Community Directive 710 (Reference 19) for the marking of classified information. NOFORN is a dissemination control marking that indicates that the resource is releasable to U.S. citizens and not

releasable to foreign nationals without the permission of the originator. If NOFORN is marked, the resource shall also be marked with a Country Determination of USA. (See Section 2.2.3.8.1)

AIS is a marking indicating that a formal determination has been made by the resource custodian that the resource may be shared via the Department of Homeland Security Automated Information Sharing (AIS) Initiative.

PII-NECESSARY-TO-UNDERSTAND-THREAT is a marking required by the AIS Initiative. Use of this marking indicates that a formal determination has been made by the resource custodian that the resource contains personal information of a specific individual or information that identifies a specific individual directly (PII) related to a cybersecurity threat as described in the Cybersecurity Information Sharing Act of 2015 (Reference 36).

NO-PII-PRESENT is also required by the AIS Initiative. Use of this marking indicates that the resource custodian has made a formal determination that there is no personal information of a specific individual or information that identifies a specific individual contained in the resource.

Generally, For Official Use Only (FOUO) is a term used to identify unclassified information of a sensitive nature. For the Department of Defense, FOUO is a dissemination control applied to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more of FOIA Exemptions 2 through 9 (Reference 17). It is addressed here for consistency with the Intelligence Community specifications and during the transition to the CUI program. FOUO disseminated Outside of the Department of Defense requires notice (front cover, first page, or at the beginning of the text): This document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act. For the Department of Homeland Security, the application of “FOUO” is governed by DHS Management Directive Number 11042.1 (Reference 24). FOUO is not used for Access Control decisions within the ESSA Community.

For an NPE, in order to receive FOUO information, the NPE must have an ATOStatus value of “ATO” and LIfeCycleStatus of “DEV”,” TEST” or “PROD”. Information system owners and authorized users have final responsibility for the Unclassified FOUO information. Enforcement of the authorization process and compliance with cybersecurity controls is necessary to safeguard Unclassified FOUO information exchanged between NPE's. Proper implementation will contain the Unclassified FOUO information within US government control, and allow access only to authorized users with need to know.

2.2.3.5 *Caveat*

This element represents specific restrictions placed on resources that are not used in access control decisions.

Name: Caveat (CVT)	**TS**	**S**	**U**
Definition: An indicator of a specific control.	As needed	As needed	As needed
Multiplicity: Multiple values permitted.			

Format: Attribute with allowable Tokens
Allowable Values: FISA
POSSIBLEPII
CISAPROPRIETARY

The FISA control marking denotes the presence of Foreign Intelligence Surveillance Act (FISA) (Reference 18) or FISA-derived information in the document. This is an informational marking only to highlight such information. Recipients of resources with the FISA control marking are responsible for ensuring that the resource is protected in conformance with the legal requirements of the FISA for limitations on use and warning displays.

The POSSIBLEPII caveat marking indicates to the recipient that the resource may contain Personally Identifiable Information (PII). Recipients are responsible for ensuring that the resource is protected according to their agencies policies related to PII. This value was included in support of the DHS Automated Information Sharing program.

The CISAPROPRIETARY caveat marking indicates that the resource must observe appropriate restrictions as requested by the originator in accordance with the Cybersecurity Information Sharing Act of 2015 (Reference 36).

2.2.3.6 *Sensitivity*

This element represents categories of data with an inherent sensitivity which requires specific restrictions in access or handling and that must be disseminated only to individuals who require the information for an authorized mission purpose. Sensitivities can apply to both classified and unclassified resources.

Executive Order 13566 (Reference 16) establishes the Controlled Unclassified Information (CUI) program to unify the current system of ad hoc categories that mark and safeguard such sensitive unclassified information. Existing practices for sensitive unclassified information remain in effect until the implementation of the CUI marking program. However, the ISA values specified below align with existing practices and the preliminary CUI marking list.

Because this attribute is characterizing the sensitivity of the data, an entity must meet all of the Sensitivity restrictions associated with the resource to gain access.

In order to restrict access based on the SENS marking, a user community must be established and governed and the custodian of the data must define the appropriate policies and determine the necessary entity attributes for access. For the Sensitivity values allowed by the ISA, some of those user communities are established. For others, they will need to be established in order to be implemented. Additional information on the organizations responsible for the governance of the community listings is included in Section 3.3 Access Groups.

In the long term, as governance processes are put in place, it is intended that this attribute be dynamically established to allow communities to be established and disestablished in support of cyber operations.

TR-83.3	If a resource has Sensitivity restrictions, then the access control mechanism shall only grant access to consumers that hold all of the corresponding entity attributes as defined by the Access Group policies.

Name: Sensitivity (SENS)	**TS**	**S**	**U**
Definition: Specifies an inherent sensitivity about the data that requires specific restrictions in access or handling.	As Needed	As Needed	As Needed
Multiplicity: Multiple values permitted.			

Format: Token of format SENS:value Allowed Values:

Value	**Description**
NTOC_DHS_ECYBER_SVC_SHARE.NSA.NSA	Enhanced Cybersecurity Services
PCII	Protected Critical Infrastructure Information
LES	Law Enforcement Sensitive Information
INT	Intelligence Information
PII	Personally Identifiable Information
TEI	Cybersecurity Targeted Entity Information
PR	Commercial Proprietary Information

Relevant values were taken from the NSA Master registry and from the Controlled Unclassified Information (CUI) List (*http://www.archives.gov/cui/registry/category-list.html*) Only those values specified in this ACS are permitted.

"Law Enforcement Sensitive" is a marking sometimes applied, separately or in addition to the marking "FOR OFFICIAL USE ONLY," by the Department of Justice and other activities in the law enforcement community, including those within the DoD. It indicates that the information was compiled for law enforcement purposes and should be afforded security in order to protect certain legitimate government interests. (Reference 17)

For more information on the DHS Protected Critical Infrastructure Information (PCII) Program, visit: http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program.

Personally Identifiable Information (PII) is defined in OMB Memorandum 07-16 as information which can be used to distinguish or trace an individual's identity such as their name, social security number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

OMB Memorandum 10-22 further states that "the definition of PII is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available, in any medium and from any source that, when combined with other available information, could be used to identify an individual." To the maximum extent possible, PII that is not relevant to the cybersecurity threat or incident should be redacted before any information is shared.

2.2.3.7 *Shareability*

The Shareability attribute allows for including flexible user-oriented access restrictions that characterize a necessary role or group that should be able to access the information. This element identifies a characteristic of the resource based on the need to share the information to a specific group within the ESSA Community. Access to the resource requires membership in a corresponding Shareability Access Group. While this may seem similar to the Sensitivity (Section 2.2.3.6) the Sensitivity marking is a dataoriented attribute that requires an entity to have permission for all Sensitivities for access to that resource. The Shareability is a user-oriented attribute that requires that an entity only need to be assigned to one of the specified Shareability Access Groups related to a resource.

If specified, an entity must meet one of the restrictions identified in this attribute to access the data.

The use of a Shareability marking and Access Groups requires that a user community within the ESSA Community be established and governed. Some of those user communities are established. For others, they will need to be established in order to be implemented. Additional information on the organizations responsible for the governance of the community listings is included in Section 3.3 Access Groups.

This attribute applies to access control decisions within the ESSA Community. In order for a data producer to place limits on ESSA Participants further sharing with other communities (for example, the Defense Industrial Base (DIB) or the Financial Industry), data producers should use the Further Sharing Attribute. If a data producer wishes to indicate that data originated from a particular group such as the DIB, the producer should use the Originator attribute and the values specified in Appendix A.

TR-83.7	If a resource has Shareability restrictions, then the access control mechanism shall only grant access to consumers that are affiliated with at least one of the Access Groups identified.

Name: Shareability (SHAR)	**TS**	**S**	**U**
Definition: Identification of the Shareability of a resource that may be released based on the determination of an originator in accordance with established disclosure procedures.	As Needed	As Needed	As Needed
Multiplicity: Multiple values permitted.			
Format: Token of format SHAR:value Allowable values: ○ NCC National Cyber Centers			

- EM Emergency Management
- LE Law Enforcement
- IC Intelligence Community

2.2.3.8 *Affiliation*

The Affiliation element (Figure 6) identifies the limitations on the distribution of the resource based on the affiliation of the user. Use of affiliation markings will limit access to the resource.

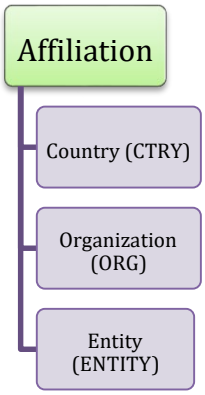

Figure 6: Affiliation

2.2.3.8.1 Country

This element identifies the country or countries to which the resource may be released based on the determination of an originator in accordance with established foreign disclosure procedures.

If specified, in order to access the resource, an entity must be a citizen of (for people) or represent (for an NPE) one of the countries listed in this attribute.

TR-83.4	If a resource has Country Disclosure restrictions, then the access control mechanism shall only grant access to consumers that are affiliated with at least one of the countries identified.

Name: Country (CTRY)	**TS**	**S**	**U**
Definition: Identification of the country or countries to which information may be released based on the determination of an originator in accordance with established foreign disclosure procedures.	As Needed	As Needed	As Needed
Multiplicity: Multiple values permitted.			
Format: Token of format: CTRY:value Allowable Values: 3-letter country code as defined in GENC standard (Reference 31).			

2.2.3.8.2 Organization

This element identifies the limitation on the distribution of the resource based on organization.

If specified, in order to access the resource, an entity must be in or assigned to (for a person) or be affiliated with (for an NPE) one of the organizations listed in this attribute.
Any limitations on access based on ORG should be made at the highest level allowable by the sharing agreements in place between organizations since the organizational values specified in Appendix A: List of Organizations are hierarchical. Access control capabilities shall understand the hierarchical nature of the ORG attribute. Access will be granted to resources marked with a higher level ORG to entities that include the high level DUTYORG and lower level organizations. For example, for a resource marked ORG:USA.DOD, access shall be granted to users with the DUTYORG:USA.DOD.DC3. The reverse is not true. Resources marked with ORG:USA.DOD.DC3 will only be allowed access to entities with DUTYORG:USA.DOD.DC3 or subordinate in the hierarchy.

TR-83.5	If a resource has Organizational Dissemination restrictions, then the access control mechanism shall only grant access to consumers that are affiliated with at least one of the organizations identified.

Name: Organization (ORG)	**TS**	**S**	**U**
Definition: Identification of the organization(s) to which information may be released based on the determination of an originator.	As Needed	As Needed	As Needed
Multiplicity: Multiple values permitted.			
Format: Token of format ORG:value Allowable Values: Listed in Appendix A: List of Organizations			

2.2.3.8.3 Entity

This element identifies the expansions or limitations on the distribution of the resource based on entity affiliation.

If specified, in order to access the resource, an entity must be in or assigned to (for a person) or be affiliated with (for an NPE) one of the entity values listed in this attribute.

TR-83.6	If a resource has Entity Dissemination restrictions, then the access control mechanism shall only grant access to consumers that are affiliated with at least one of the Entity values identified.

Name: Entity (ENTITY)	**TS**	**S**	**U**
Definition: Identification of the entities to which information may be released based on the determination of an originator.	As Needed	As Needed	As Needed
Multiplicity: Multiple values permitted.			

Format: Token of format ENTITY:value
Allowable Values: MIL, GOV, CTR, SVR, SVC, DEV, NET
(These values have a one-to-one correspondence to the Entity Attribute Entity Type in the Unified Identity Attribute Set (Reference 6))

3 ISA Entity Attributes

Entity attributes are characteristics about the person entity (PE) or non-person entity (NPE) that is requesting access to an information resource. An entity may have one or more personas as identified by unique credentials and separate sets of attribute values. For example, a contractor who is also a reserve military member will have two credentials that identify a separate set of attributes for each of the two roles.

TR-20	*"All users and non-person entities (NPEs) shall have the identification and authorization metadata listed in Table 13: Summary of ISA Entity Attributes" (Reference 3)*
TR-20.2	ISA access control mechanisms shall make access control decisions using only the entity attributes defined in the ISA ACS.

Attributes are indicated as Required, Optional, or Ignored in Table 3-1 for the applicable network classification level. As stated before, this document does not prescribe all access control attributes that an organization needs internal to their enterprise systems. Additionally, this section does not specify an Entity Attribute Management Capability. ESSA Information Sharing Participants and Shared Capability Providers must establish capabilities that support the use of ISA Entity Attributes for access control.

In cases where attribute names and values differ in internal implementations, they must be transformed or derived to match this specification. For each ISA entity attribute, likely mappings are identified for this type of transformation from the IC Enterprise Attribute Set (Reference 6), the DoD EIAS (Reference 7), and the DoJ GFIPM (Reference 8) in Appendix C: Deltas between ISA ACS Entity Attributes and UIAS/EIAS/GFIPM .

The following definitions are used in Table 3-1 for Required, Optional, and Ignored:

- *Required* – Entities seeking access to a resource must provide the attribute. Therefore, the authors of access rules can expect to have that minimum set of information for use in the decision. "Required" does not mean that the attribute must be used in making the access decision.
- *Optional* – Entities seeking access to a resource may provide the attribute, but it can also be left empty. Therefore, the access rules may require that information for use in the decision. If the attribute is considered necessary to gain access to a resource but is not provided, then access is denied.
- *Ignored* – The attribute is explicitly not used in making access decisions at that classification level.

Table 3-1: Summary of ISA Entity Attributes

ISA Entity Attribute Name	SAML v2.0 Attribute Identifier urn:isa:acs:ns:v3.0:	Multiplicity	Person or NPE	Top Secret Network	Secret Network	Unclassified Network
Digital Identifier	subjectDN	single	Both	Required	Required	Required
Admin Organization	organization	single	Both	Required	Required	Required
Authority Category	authority	multiple	Both	Optional	Optional	Optional
Access Group	assignment	multiple	Both	Optional	Optional	Optional
ATO Status	certification	single	NPE	Required	Required	Required
Authorized IC Person*	attribute	single	Person	Required	Ignored	Ignored
Clearance	clearance	single	Both	Required	Required	Ignored
Country of Affiliation	country	multiple	Both	Required	Required	Required
Duty Organization	dutyStation	single	Both	Required	Required	Required
Entity Type	category	single	Both	Required	Required	Required
Fine Access Controls	clearance:control	multiple	Both	Required	Ignored	Ignored
Is IC Member*	memberOf	single	Both	Required	Ignored	Ignored
Life Cycle Status	position	single	NPE	Required	Required	Required

** These entity attributes are specifically designed for the IC and are not applicable outside of that community.*

3.1 Admin Organization

The Admin Organization attribute specifies the home or administrative organization with which the entity (person or non-person) is associated. For NPEs, the administrative organization is the one that controls the administration of the NPE when in use.

TR-20.3	Each person entity and non-person entity (NPE) shall have an Admin Organization attribute accessible by ISA access control mechanisms.

Name: AdminOrganization urn:isa:acs:ns:v3.0:organization		**TS**	**S**	**U**
Definition: There must be a value that reflects the home organization of the entity		Required	Required	Required
P or NPE: Both	Multiplicity: Single value permitted.			

UIAS Field: AdminOrganization EIAS Field: ADM_ORG_CD GFIPM Field: Employer Name or Owner Agency Name (text field – may need to be mapped to allowable values)
Format: String Allowable values listed in IC Standard: Controlled Vocabulary Enumeration for USAgency (USAgencyCVEnums) (Reference 29)

3.2 Authority Category

The Authority Category attribute specifies the authority under which the entity is authorized to access a resource protected by a Logical Authority Category.

Name: AuthorityCategory urn:isa:acs:ns:v3.0:authority		**TS**	**S**	**U**
Definition: Specifies the authority under which the entity is authorized to access a resource.		Optional	N/A	N/A
P or NPE: Both	Multiplicity: Multiple values permitted.			
UIAS Field: AuthorityCategory EIAS Field: None GFIPM Field: None				
Format: String Allowable values listed in NSA's Master Data Registry.				

3.3 Access Groups

Access Groups are attributes assigned to individuals who require specific controlled information for an authorized mission purpose. The use of an Access Group requires that a user community be established and governed and an administrative mechanism for the assignment and management of the attributes be implemented.

The set of values for the Access Group attribute assumes that the policy rule application will compare Access Group values directly to Sensitivity and Shareability restrictions. If the Access Group assignment capability is not available, other policy rules may be required to support access to resources tagged with Sensitivity and Shareability restrictions. A discussion of possible interim policy applications for Sensitivity and Shareability restrictions is included in Section 4.

The Protected Critical Infrastructure Information program specifies controls for PCII resources. However, there is not currently an entity attribute management system in place to assign this attribute to PE and NPEs. If PCII resources are required to be shared by ESSA Information Sharing Participants prior to the assignment of entity attributes, DHS will need to establish the policy rules under which these resources can be accessed.

There is an ongoing effort to provide governance for unclassified information that requires additional controls as required by Executive Order 13556, Controlled Unclassified Information (Reference 16) Some of the groups named below are named to align with the Controlled Unclassified Information (CUI) List (*http://www.archives.gov/cui/registry/category-list.html*) where the data described by the CUI type require membership in a particular group in order to permit access.

<table>
<tr><td colspan="2">Name: AccessGroups urn:isa:acs:ns:v3.0:assignment</td><td>TS</td><td>S</td><td>U</td></tr>
<tr><td colspan="2">Definition: Specifies a particular group of which the entity is a member which, through the application of policy rules, may allow access to sensitive or shared resources. Nothing is returned when an entity has no LogicalAccessGroups.</td><td rowspan="2">Optional</td><td rowspan="2">Optional</td><td rowspan="2">Optional</td></tr>
<tr><td>P or NPE: Both</td><td>Multiplicity: Multiple values permitted.</td></tr>
<tr><td colspan="5">UIAS Field: The IC is considering the addition of a “group” attribute.
EIAS Field: None
GFIPM Field: None</td></tr>
<tr><td colspan="5">Format: String
Allowable Values: ○ PCII Authorized Protected Critical Infrastructure Information Recipients ○ PII Personally Identifiable Information
○ PR Proprietary
○ TEI Authorized Cybersecurity Targeted Entity Information Recipients ○ NTOC_DHS_ECYBER_SVC_SHARE.NSA.NSA Enhanced Cybersecurity Services ○ NCC Federal Cyber Center Entities ○ EM Emergency Management Entities
○ LE Law Enforcement Entities</td></tr>
</table>

3.4 ATO Status

Authority to Operate (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a NPE at a particular level of security in a particular environment and explicitly accepts the risk to agency operations. The ATO is signed after a Certification Agent (CA) certifies that the system has met and passed all requirements to become operational. The ATO Status should be used in conjunction with the Life Cycle Status attribute to fully determine the status of the NPE.

TR-20.4	Each non-person entity (NPE) shall have an Authority to Operate (ATO) Status attribute accessible by ISA access control mechanisms.

Name: ATOStatus urn:isa:acs:ns:v3.0:certification	**TS**	**S**	**U**

Definition: The formal status of a NPE related to its operation as declared by a Designated Approving Authority (DAA)..		Required	Required	Required
P or NPE: NPE	Multiplicity: Single value permitted.			
UIAS Field: ATOStatus EIAS Field: N/A GFIPM Field: None				
Format: Boolean Allowable Values: True or False				

3.5 Authorized IC Person

An Authorized IC Person (AICP) is defined by Intelligence Community Directive 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community,* (Reference 25) as follows:

> "A U.S. person employed by, assigned to, or acting on behalf of an IC element who, through the course of their duties and employment, has a mission need and an appropriate security clearance for information collected or analysis produced. Authorized IC personnel shall be identified by their IC element head and shall have discovery rights to information collected and analysis produced by all elements of the IC. The term may include contractor personnel."

This attribute reflects whether a person has been identified by their IC element head to act as an AICP. Under ICD 501, only users employed by, assigned to, or acting on behalf of an IC element may be AICPs. Note that there are many IC members but relatively few are designated as AICPs.

Note: This attribute is dependent upon '*Is IC Member*' (Section 3.12). '*Authorized IC Person*' can only be applied to persons that are members of the IC as defined in the '*Is IC Member*'.

TR-20.5	Each person entity shall have an Authorized IC Person (AICP) Status attribute at the TS network level accessible by ISA access control mechanisms.

Name: AICP urn:isa:acs:ns:v3.0:attribute		**TS**	**S**	**U**
Definition: The value is returned when the person is an Authorized IC Person (AICP) as described in ICD 501.		Required	Ignored	Ignored
P or NPE: Person	Multiplicity: Single value permitted.			
UIAS Field: AICP EIAS Field: None GFIPM Field: None				
Format: Boolean Allowable Values: True or False				

3.6 Clearance

The Clearance attribute specifies the entity's security clearance level for a person entity, or the highest security classification of information that can be handled by an NPE as specified in the accredited System Security Plan. Clearance is used for access control decisions to classified resources. This attribute does not indicate that an entity holds an "interim" clearance. If there is no value for Clearance then the entity can only access unclassified resources.

TR-20.6	Each person entity and non-person entity (NPE) shall have a Clearance attribute on classified network levels accessible by ISA access control mechanisms.

<table>
<tr><td colspan="2">Name: Clearance
urn:isa:acs:ns:v3.0:clearance</td><td>TS</td><td>S</td><td>U</td></tr>
<tr><td colspan="2">Definition: Reflects the clearance level of the entity in accordance with the US control system.</td><td rowspan="2">Required</td><td rowspan="2">Required</td><td rowspan="2">Ignored</td></tr>
<tr><td>P or NPE: Both</td><td>Multiplicity: Single value permitted.</td></tr>
<tr><td colspan="5">UIAS Field: Clearance
EIAS Field: JPAS_ACS_CD, JPAS_ELIG_CD
GFIPM Field: Clearance Code</td></tr>
<tr><td colspan="5">Format: String Allowable
Values:
<u>Value</u> — <u>Definition</u>
C — Confidential
S — Secret
TS — Top Secret</td></tr>
</table>

3.7 Country of Affiliation

The Country of Affiliation attribute specifies the entity's affiliation with a country or countries. In the case of person entities, this is the identifier of the entity's country or countries of citizenship. In the case of non-person entities, this represents the citizenship of the administrator or the country affiliation of the organization in control of the non-person entity.

Country of Affiliation is multi-valued, since an entity could possibly have multiple citizenships (e.g., "dual citizenship") relevant for access control decisions.

TR-20.7	Each person entity and non-person entity (NPE) shall have a Country of Affiliation attribute accessible by ISA access control mechanisms.

Name: CountryOfAffiliation urn:isa:acs:ns:v3.0:country	**TS**	**S**	**U**

Definition: Reflects the citizenship of the person or the citizenship of the administrator(s) and/or the organization(s) in control of the NPE.		Required	Required	Required
P or NPE: Both	Multiplicity: Multiple values permitted.			
UIAS Field: CountryOfAffiliation EIAS Field: CTZP_CTRY_CD GFIPM Field: Citizenship Code (uses 2-letter Country Code, may need to be mapped to allowable 3 or 4letter codes)				
Format: String Allowable Values: 3-letter country code as defined in GENC. The GENC Standard Edition 1.0 (Reference 31) is the US Government implementation of ISO 3166-1 that conforms to US Board on Geographic Names and US Government recognition policy. Example Value: USA				

3.8 Digital Identifier

A Digital Identifier is the representation that uniquely identifies a person or non-person entity's persona. For the ESSA community a Digital Identifier is the primary key to an attribute repository and therefore is required. A PKI certificate's subject Distinguished Name (DN) is a string representation that uniquely identifies the entity within a specific PKI directory service and is one source of a unique Digital Identifier.

TR-20.8	Each person entity and non-person entity (NPE) shall have a Digital Identifier accessible by ISA access control mechanisms.

Name: DigitalIdentifier subjectDN		**TS**	**S**	**U**
Definition: A representation that uniquely identifies a persona entity or non-person entity persona. Acceptable sources include the Distinguished Name (DN) from the entity's Public Key Infrastructure (PKI) Certificate.		Required	Required	Required
P or NPE: Both	Multiplicity: Single value permitted.			
UIAS Field: DigitalIdentifier EIAS Field: DOD_EDI_PN_ID GFIPM Field: Electronic Identity Id				
Format: String Example Values: • Person Example: cn=Doe John A jdoe, ou=DNI, o=U.S Government, c=US • NPE Example: cn=webserver.dni.ic.gov, ou=DNI, o=U.S. Government, c=US				

3.9 Duty Organization

The Duty Organization attribute specifies the organization which the entity (person or non-person) is representing.

The Duty Organization may differ from the Admin Organization for a person entity in cases where the entity is detailed from their home or administrative agency to another agency for a Joint Duty assignment or other rotation.

TR-20.9	Each person entity and non-person entity (NPE) shall have a Duty Organization attribute accessible by ISA access control mechanisms.

Name: DutyOrganization urn:isa:acs:ns:v3.0:dutyStation		**TS**	**S**	**U**
Definition: Reflects the assigned organization of the entity (entity may be detailed from their home agency to another agency for a Joint Duty assignment).		Required	Required	Required
P or NPE: Both	Multiplicity: Single value permitted.			
UIAS Field: DutyOrganization EIAS Field: DUTY_DOD_OCC_CD GFIPM Field: Assignment Agency Name (text field – may need to be mapped to allowable values)				
Format: String Allowable values: Listed in Appendix A: List of Organizations				

3.10 Entity Type

The Entity Type attribute indicates the type of affiliation that the entity (person or non-person) has with their administrative organization. Further clarification on NPE Entity attribute definitions can be found in the Unified Identity Attribute Set (UIAS) (Reference 6).

TR-20.10	Each person entity and non-person entity (NPE) shall have an Entity Type attribute accessible by ISA access control mechanisms.

Name: EntityType urn:isa:acs:ns:v3.0:category		**TS**	**S**	**U**
Definition: Reflects the type affiliation with the administrative organization of the entity.		Required	Required	Required
P or NPE: Both	Multiplicity: Single value permitted.			
UIAS Field: EntityType EIAS Field: DOD_ASSOC_CD GFIPM Field: Organization General Category Code				

Format: String Allowable Values:

Value	Definition	Applicable Entity
MIL	Military service member	Person
CTR	Contractor	Person
GOV	Government civilian employee	Person
SVR	Server	Non-Person
SVC	Service, Widget, Application, Software, etc.	Non-Person
DEV	End-point device	Non-Person
NET	Network device	Non-Person

3.11 Fine Access Controls

The Fine Access Controls attribute is based on the Fine Access Control (FAC) attribute included in the Intelligence Community Information Security Markings (Reference 26). This attribute includes Sensitive Compartmented Information (SCI) Control Systems and Compartments, Special Access Programs/Special Access Restrictions, Atomic Energy Act, DoD Critical Nuclear Weapons Design Information (CNWDI) and Department of Energy compartments which an entity (person or non-person) is authorized to access or process. It also includes the caveats associated with the clearances, where appropriate. An NPE must be accredited to handle SCI resources as specified in its System Security Plan.

TR-20.11	Each person entity and non-person entity (NPE) shall have a Fine Access Controls attribute at the TS network level accessible by ISA access control mechanisms.

Name: FineAccessControls urn:isa:acs:ns:v3.0:clearance:control		**TS**	**S**	**U**
Definition: Reflects the fine grain access control permissions granted to the entity.		Required	Ignored	Ignored
P or NPE: Both	Multiplicity: Multiple values permitted.			
UIAS Field: FineAccessControls EIAS Field: None GFIPM Field: None				
Format: String Allowable Values: Values listed in the Controlled Vocabulary Enumeration for FAC, December 22, 2014 (Reference 27)				

3.12 Is IC Member

The Is IC Member attribute is a flag that reflects whether the entity (person or non-person) is a member of the Intelligence Community as defined by EO 12333 (Reference 28) , where an IC member is “a person employed by, assigned or detailed to, or acting for an element within the IC.”

TR-20.12	Each person entity and non-person entity (NPE) shall have an Is IC Member attribute at the TS network level accessible by ISA access control mechanisms.

<table>
<tr><td colspan="3">Name: isICMember urn:isa:acs:ns:v3.0:memberOf</td><td>TS</td><td>S</td><td>U</td></tr>
<tr><td colspan="3">Definition: Reflects whether or not the entity is a member of the Intelligence Community as defined by EO12333.</td><td rowspan="2">Required</td><td rowspan="2">Ignored</td><td rowspan="2">Ignored</td></tr>
<tr><td>P or NPE: Both</td><td colspan="2">Multiplicity: Single value permitted.</td></tr>
<tr><td colspan="6">UIAS Field: isICMember
EIAS Field: None
GFIPM Field: None</td></tr>
<tr><td colspan="6">Format: Boolean
Allowable Values: True or False</td></tr>
</table>

3.13 Life Cycle Status

The Life Cycle Status attribute indicates the life cycle phase in which the entity is operating, and can be used for access control to protected resources. This attribute is only applicable for NPEs. The Life Cycle Status should be used in conjunction with the ATO Status attribute to fully determine the status of the NPE. (Reference 6)

TR-20.13	Each non-person entity (NPE) shall have a Life Cycle Status attribute accessible by ISA access control mechanisms.

<table>
<tr><td colspan="3">Name: LifeCycleStatus urn:isa:acs:ns:v3.0:position</td><td>TS</td><td>S</td><td>U</td></tr>
<tr><td colspan="3">Definition: Indicates the life cycle phase in which the entity is operating.</td><td rowspan="2">Required</td><td rowspan="2">Required</td><td rowspan="2">Required</td></tr>
<tr><td>P or NPE: NPE</td><td colspan="2">Multiplicity: Single value permitted.</td></tr>
<tr><td colspan="6">UIAS Field: LifeCycleStatus
EIAS Field: N/A
GFIPM Field: None</td></tr>
</table>

Format: String Allowable Values:

Value	Definition
DEV	Development
TEST	Test
PROD	Production
SUNSET	Sunset/Retired

4 ISA Access Control Policy Rules

ISA Access Control Policy Rules specify to the intended use of the ISA Resource and Entity attributes to render an access decision. Table 4-1 defines the intended relationships between ISA Entity and Resource Attributes. Please note that all access and dissemination decisions depend on the specific facts involved in each case. These policy rules are provided to demonstrate how resource markings and entity attributes are applied to make access decisions but they should not be used to make substantive policy determinations. In all cases, entities responsible for encoding policy rules should also consult with legal counsel and appropriate compliance personnel. Note also that in some cases resource attributes are provided for identification or handling instructions. While these may inform access decisions, they do not have entity attribute counterparts. Appendix E: Access Control Rule Set Example provides a pseudo code example of implementation of the policy rules in Table 4-1.

Table 4-1: Relationship between ISA Resource Attributes and ISA Entity Attributes

ISA Resource Attributes	ISA Entity Attributes	Policy Rule	Policy Rule Application
Classification	Clearance	Clearance must be same level or higher than Classification	<=
SCI Controls	Fine Access Controls	All values from Resource Attributes must be found in Entity Attribute list	AND
Logical Authority Category	Authority Category	All values from Resource Attributes must be found in Entity Attribute list	AND
Sensitivity	Access Group	All values from Resource Attributes must be found in Entity Attribute list	AND
Shareability	Access Group	One of the values from the Resource Attributes must be found in the Entity Attribute list	OR
Country	Country of Affiliation	One of the values from the Resource Attributes must be found in the Entity Attribute list	OR
Organization	Duty Organization	One of the values from the Resource Attributes must be found in the Entity Attribute Duty list	OR

Entity	Entity Type	One of the values from the Resource Attributes must be found in the Entity Attribute list	OR
N/A[9]	ATO Status	All non-person entities (NPEs) shall have an Authority to Operate (ATO) Status attribute of "true".	May be applied for access to all resources
ISA Resource Attributes	**ISA Entity Attributes**	**Policy Rule**	**Policy Rule Application**
N/A	Life Cycle Status	All non-person entities (NPEs) shall have a Life Cycle Status attribute accessible by ISA access control mechanisms.	May be applied for access to all resources

4.1 Access Control Policy Rule Limitations

The use of Access Groups as entity attributes requires that a user community be established and governed and an administrative mechanism for the assignment and management of the attributes implemented. In initial implementations of the ISA, this capability may not be available. In Table 4-1, the policy rules compare the set of values for the Access Group directly to Sensitivity and Shareability. If the Access Group assignment capability is not available, other policy rules may be required to support access to resources tagged with Sensitivity and Shareability restrictions.

Until an Access Group management capability is available, the following policies address the presence of several Shareability and Sensitivity resource attributes:

- SENS:INT and SHAR:IC require that the entity attribute IsICMember=true
- SHAR:NCC require that the entity Duty Org have a value of an Organization that is one of the National Cyber Centers

The following Sensitivity and Shareability restrictions cannot be enforced and should not be used without the establishment of the Access Group capability:

- SENS:PCII
- SENS:LES
- SENS:PII
- SENS:TEI
- SENS:PR
- SHAR:EM
- SHAR:LE

Please note that access control capabilities must be able to understand the hierarchical nature of the ORG attribute.

[9] While there are no direct parallels to ATO Status and Life Cycle Status when tagging at the individual pieces of data, it is expected that access rules will check these attributes at a system level before interfacing with the NPE

requesting access.

5 ISA Access Control Use Cases

5.1 Use Case 1: Access Granted to Cybersecurity Data

A civilian employee of the Department of Homeland Security (DHS) works within the National Cybersecurity and Communications Integration Center (NCCIC), which is an ISA Participant. This person is requesting access to classified information about malware held by the National Security Agency (NSA). NSA has determined that this information is releasable to civilian, federal contractors, and military personnel at the six Federal Cybersecurity Centers, which are members of the NCC Access Group. Furthermore, classified data will only be shared on the TS network if the entity requesting access presents a valid PKI certificate.

The access decision in this scenario is represented in Table 5-1. After the entity has been authenticated by presenting a valid PKI certificate, the NSA authorization service requests the attributes of the NCCIC employee. The DHS attribute service returns the values associated with the particular NCCIC employee. The NSA authorization service checks the following rules:

a) Data classified as Top Secret can only be shared with entities with a Top Secret Clearance.
b) This data can only be shared with entities in the National Cyber Centers (NCC) Access Group.
c) Data marked for dissemination to GOV, CTR, or MIL can only be shared with person entities of the GOV, CTR, or MIL Entity Type.

Table 5-1: Use Case One – Access Granted to Cybersecurity Data

ISA Entity Attributes	DHS Employee	Application of Policy Rules	Resource Information	ISA Resource Attributes
Digital Identifier	Valid			
Clearance	TS	☑ - Rule (a)	TS	Classification (CLS)
Fine Access Controls				SCI Controls (SCI)
Authority Category				Logical Authority Categories (LAC)
Access Group	NCC	☑ - Rule (b)	NCC	Shareability (SHAR)

				Sensitivity (SENS)
Country of Affiliation	USA			Country (CTRY)
Duty Organization	USA.DHS.NCCIC			Organization (ORG)
Entity Type	GOV	☑ - Rule (c)	GOV, CTR, or MIL	Entity (ENTITY)
ATO Status	N/A			
Life Cycle Status	N/A			
Authorized IC Person	No			
Is IC Member	No			

Based on this scenario, ***the entity should be granted access*** to the specific information. Note that a similar exchange would also authenticate and authorize the system that the DHS employee is using to verify that it, as an NPE, is also allowed to access the classified data.

5.2 Use Case 2: Access Privilege

This Use Cases addresses the case where usage restrictions are placed on the resource limiting the actions that can be taken after an access control decision has been made. In this Use Case, a recipient of the resource can take a particular action but only after getting permission from the custodian. FBI sends a report on a malicious IP address out at an Unclassified For Official Use Only (FOUO) level but knows there is some law enforcement activity going on that requires that further actions taken on the address must not alert the malicious actor of knowledge of the malicious activity. Participants can monitor traffic to and from the IP but they cannot take a NETDEF action. If everyone takes a NETDEF action and blocks this IP address, then the malicious actor would know it and move. If however, there is additionally a sensitive military operation going on requiring additional action based on the information, the military unit can contact the FBI and request permission to do a NETDEF action given their particular situation. FBI might say yes, but then again, FBI might still say no if their equities review process indicated this would compromise the mission.

The following rules are applied and the initial access decision in this scenario is represented in Table 5-2.

a) Data classified as Unclassified can be shared with entities with or without a Clearance.

Table 5-2: Use Case Two – AccessPrivilege

ISA Entity Attributes	MIL Member	Application of Policy Rules	Resource Information	ISA Resource Attributes
Digital Identifier	Valid			
Clearance	TS	☑ - Rule (a)	U	Classification (CLS)
Fine Access Controls				SCI Controls (SCI)
Authority Category				Logical Authority Categories (LAC)

Access Group	NCC			Shareability (SHAR)
		☑ - Rule (b)		Sensitivity (SENS)
			FOUO	Formal Determination (FD)
Country of Affiliation	USA			Country (CTRY)
Duty Organization	USA.DOD			Organization (ORG)
Entity Type	GOV			Entity (ENTITY)
ATO Status	N/A			
Life Cycle Status	N/A			
Authorized IC Person	No			
Is IC Member	No			

Based on this scenario, ***the entity should be granted access*** to the specific information. Note that a similar exchange may also authenticate and authorize the system that the user is using to verify that it, as an NPE, is also allowed to access the data.

Following the access control decision, the following rules are levied to limit action based on access to the resource:

a) This data may only be used for monitoring and analysis.

b) Special request may be made for additional permissions.

Restrictions following access are specified with Access Privilege markings. In this use case, the markings would set the default AccessPrivilege to "deny" and include specific permissions for all user entities to conduct intelligence activities. In addition, the privilegeAction of REQUEST would indicate that a special request may be made by the receiver to conduct additional actions. The markings would include:

- <PolicyRef>urn:isa:policy:acs:ns:v3.0?privdefault=deny&sharedefault=permit
- <privilegeAction>INTEL
- <privilegeScope>ALL
- <ruleEffect>permit
- <privilegeAction>DSPLY
- <privilegeScope>ALL
- <ruleEffect>permit
- <privilegeAction>REQUEST
- <privilegeScope>ALL
- <ruleEffect>permit

5.3 Use Case 3: PUBREL and Portion Marking

In this use case, NSA requests a cyber report from DHS. The highest classification of the report is Secret. Some elements of the report were previously released to the public through DHS US-CERT public notification process. Additional information on the application of ISA markings to portion mark STIX™ documents is available in the ISA STIX™ Profile Description (Reference 21).

The following rules are applied and the access decision in this scenario is represented in Table 5-3.

a) Data classified as Secret can be shared with entities with a clearance of Secret or Top Secret.

Table 5-3: Use Case Three – PUBREL and Portion Marking

ISA Entity Attributes	Requestor	Application of Policy Rules	Resource Information	ISA Resource Attributes
Digital Identifier	Valid			
Clearance	TS	☑ - Rule (a)	S	Classification (CLS)
Fine Access Controls				SCI Controls (SCI)
Authority Category				Logical Authority Categories (LAC)
Access Group	NCC		Some elements of the report are PUBREL	Shareability (SHAR)
				Sensitivity (SENS)
				Formal Determination (FD)
Country of Affiliation	USA			Country (CTRY)
Duty Organization	USA.NSA			Organization (ORG)
Entity Type	GOV			Entity (ENTITY)
ATO Status	N/A			
Life Cycle Status	N/A			
Authorized IC Person	Yes			
Is IC Member	Yes			

Based on this scenario, ***the entity should be granted access*** to the specific information.

Upon access, review of the document would show that sub-components of the document may be marked with less restrictive markings. In this case, the Control Set for the resource would be marked:

<ControlSet>CLS:S

Sub-components that were publically releaseable would include the following elements:

<ControlSet>CLS:U

<FormalDetermination> PUBREL

<ReleasedBy>Authority

<ReleaseDate>YYYY-MM-DD

5.4 Use Case 4: Analytic NPE

A non-person entity (NPE) analytic owned by the US Cyber Command Joint Operations Center (JOC) is operating on a production system that has a valid ATO. This analytic is a standing query that furnishes information to a publish/subscribe service. It is leveraging a web service to request access to unclassified indicators accessed via the ISA Unclassified Malware and Indicators Storefront, managed by the Defense Cyber Crime Center (DC3). DC3 allows only US Government entities to access this storefront. Furthermore, DC3 will only allow access if the entity requesting access presents a valid PKI certificate, has a valid ATO, and is a production system.

The access decision in this scenario is represented in Table 5-4. After the entity has been authenticated by presenting a valid PKI certificate, DC3 leverages the DoD authorization service to request the attributes of the USCYBERCOM NPE. The DoD authorization service returns the values associated with the particular USCYBERCOM NPE. The DoD authorization service checks the following rules:

a) Data marked for dissemination to USA.USG can only be shared with entities with a Duty Organization that is a member of the US Government.

b) Data marked for dissemination to MIL, CTR, GOV, SVR, SVC, DEV, and NET can only be shared with entities with an Entity Type of MIL, CTR, GOV, SVR, SVC, DEV, or NET.

c) Production DC3 systems will only share with NPEs with an ATO Status of True.

d) Production DC3 systems will only share with NPEs with a Life Cycle Status of PROD.

Table 5-4: Use Case Four – Analytic NPE

ISA Entity Attributes	USCYBERCOM NPE	Application of Policy Rules	DC3 Indicator	ISA Resource Attributes
Digital Identifier	Valid			
Clearance			U	Classification (CLS)
Fine Access Controls				SCI Controls (SCI)
Authority Category				Logical Authority Categories (LAC)
Access Group	NCC			Shareability (SHAR)
				Sensitivity (SENS)
Country of Affiliation	USA			Country (CTRY)

Duty Organization	USA.DOD.USCYBERCOM	☑ - Rule (a)	USA.USG	Organization (ORG)
Entity Type	SVC	☑ - Rule (b)	MIL, CTR, GOV, SVR, SVC, DEV, NET	Entity (ENTITY)
ATO Status	True	☑ - Rule (c)	ATO	*Required by DC3 Policy*
Life Cycle Status	PROD	☑ - Rule (d)	PROD	*Required by DC3 Policy*
Authorized IC Person	N/A			
Is IC Member	No			

Based on this scenario, ***the entity should be granted access*** to the specific information.

5.5 Use Case 5: Access Denied to Law Enforcement Data

In this use case, the entity is a military employee of US Cyber Command JOC, which is an ISA Participant. This person is searching through unclassified FOUO information about malware held by the Federal Bureau of Investigation (FBI). While the search returns other results, the FBI has tagged this particular information as law enforcement sensitive because it is tied to an active investigation.

The access decision in this scenario is represented in Table 5-5. After the entity has been authenticated by presenting a valid PKI certificate, the FBI leverages the FBI authorization service to request the attributes of the JOC employee from the DoD authorization service. The DoD authorization service returns the values associated with the particular JOC employee. The FBI authorization service checks the following rules:

a) Law Enforcement data can only be shared with entities in the LES Access Group.

b) Data marked for dissemination to USG or SLTT can only be shared with entities with a Duty Organization that is either SLTT or a member of the USG

c) Data marked for dissemination to MIL, CTR, and GOV can only be shared with entities with an Entity Type of MIL, CTR, or GOV

Table 5-5: Use Case Five – Access to Law Enforcement Data Denied

ISA Entity Attributes		Application of Access Rules		ISA Resource Attributes
Digital Identifier	Valid			
Clearance	U		U	Classification (CLS)
Fine Access Controls				SCI Controls (SCI)

Authority Category				Logical Authority Categories (LAC)
Access Group	NCC			Shareability (SHAR)
		☒ - Rule (a)	LES	Sensitivity (SENS)
Country of Affiliation	USA			Country (CTRY)
Duty Organization	USA.DOD.USCYBERCOM	☑ - Rule (b)	USA.USG	Organization (ORG)
Entity Type	MIL	☑ - Rule (c)	MIL, CTR, GOV, SVR, SVC, DEV, NET	Entity (ENTITY)
ATO Status			ATO	
Life Cycle Status			PROD	
Authorized IC Person	N/A			
Is IC Member	No			

Based on this scenario, ***the entity should not be granted access*** to the specific information because Access Rule (a) was not satisfied.

6 Open Issues

The following access control issues remain to be resolved:

- *Authentication* – Will the Intelligence Community Information Technology Enterprise (IC ITE) negotiated trust relationship be available for all ISA Participants to leverage (at the TS level)? Do all IC organizations utilize the complete list of trusted CAs or do they cherry pick who they want to share with?
- *Authentication* – Will the DoD Interoperability Root allow two way authentications with the Federal Bridge CA? Will the authentication be extended to the staff of the National Security Council (NSC) hardware certificates in addition to software certificates?
- *Cross-organizational Agreements* – What cross-organizational agreements must be in place to establish a Access Group that is not based on a legal authority? There is limited existing capability to implement Access group restrictions. The User Attributes services will need to provide the correct user attributes/entitlements. Is there a plan for an entitlement service? The service needs to be flexible to support the establishment of ad hoc establishment and disestablishment of communities.
- *Cross-organizational Agreements* – What cross-organizational agreements are needed to enable subsequent sharing? Is there a common use of handling instructions (or minimum tagging) for subsequent sharing of formal vs. interim vs. advisories vs. unreviewed data? Are there agreements in place today and does ABAC technology change them?
- *Cross-organizational Agreements* – What coordination needs to be done regarding retention policies?
- *Implementation* – Can a back-end attribute exchange also support machine-to-machine addition and removal of attribute values? For example, DHS would manage the Critical Infrastructure Access Group and may want someone whose attributes are managed by another organization to have that attribute. In this example, how would DHS drive that change?
- *Ad hoc Cross-Organizational Communities of Interest (CCOI)* – Is there a need for a flexible CCOI implementation that can create and end CCOIs based on active events?
- *Implementation* – Since the values for the Access Groups come from multiple sources, what additional coordination is needed to fully develop and deconflict the allowable values vocabulary for cyber information sharing?
- *Implementation* – How will the ACS address evolution in marking standards? As specifications are updated, it will be possible to have two or more versions of acceptable markings active in shared data at any one point in time. Policies must accommodate such evolution.
- *Implementation* - Analysts within each organization must be appropriately trained to ensure they are implementing the policies outlined in the ACS correctly. How will training be handled to ensure analysts within each organization fully understand how to implement the policies and requirements outlined in this document?

7 Conclusion

This ISA Access Control Specification supplements the Information Requirements in the *ISA SSA Requirements Document* by providing a common set of entity and resource attributes that meet the needs of the ESSA Information Sharing Participant Community. With continued investments in tactical,

operational, and strategic implementations of the ISA, the initiative continues to engage stakeholders in identifying requirements in aligning current doctrine, operational engagement plans, and/or policy of their organizations to facilitate executing the set of capabilities necessary for Enhanced Shared Situational Awareness (ESSA) to enable Integrated Operational Action (IOA).

References

1. NIST Special Publication 800-162 “Guide to Attribute Based Access Control (ABAC) Definition and Considerations”, January 2014.
2. ISA Framework, September 30, 2011
3. ISA SSA Requirements Document, Oct 21, 2013
   - https://max.omb.gov/community/x/MRV6KQ
4. ISA Technical Implementation Plan, July 18, 2013
   - https://max.omb.gov/community/x/MRV6KQ
5. Federal Identity Credential and Access Management (FICAM) Roadmap and Implementation Guidance
   - http://www.idmanagement.gov/documents/ficam-roadmap-and-implementationguidance
6. IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set, Version 3 (September 6, 2013)
   - http://www.dni.gov/index.php/about/organization/chief-information-officer/idamauthorization-attribute-set
7. Enterprise Identity Attribute Service (EIAS) User Integration Guide (November 15, 2011)
   - https://www.intelink.gov/go/YCKQa0r (*Note: Intelink-U account required)*
8. DoJ Global Federated Identity and Privilege Management
   - http://gfipm.net/standards/metadata/2.0/user.html
9. Intelligence Community Enterprise Data Header (IC-EDH) (July 17, 2012)
   - http://www.dni.gov/files/documents/CIO/ICEA/IC-EDHPublic.zip
10. National Institute of Standards and Technology (NIST) Special Publication 800-63-1, Electronic Authentication Guideline, December 2011
    - http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
11. Structured Threat Information eXpression (STIX)
    - http://stix.mitre.org/
12. Enterprise Data Header Abstract Data Definition (ADD) version 1.0, 20 June 2014.
    - https://community.max.gov/download/attachments/699566316/EDH_ADD.pdf?version=1&modificationDate=1413902608344&api=v2
13. Smart Data Enterprise Data Header Data Encoding Specification (DES) Version 2.0, July 2014.
    - https://community.max.gov/download/attachments/699566316/SDEDH_DES.txt?version=1&modificationDate=1405517925189&api=v2
14. Smart Data Enterprise Data Header (EDH) Implementation Profile for the U.S. Intelligence Community
15. Smart Data Enterprise Data Header (EDH) Implementation Profile for the Cyber Community https://community.max.gov/download/attachments/699566316/SD-EDH_Profile_Cyber.pdf?version=1&modificationDate=1427737507998&api=v2
16. Executive Order 13556, Controlled Unclassified Information, November 4, 2010
    - http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf

17. DoD Information Security Manual, DoDM 5200.01, Volumes 1-4. February 24, 2012 (Formerly CAPCO Manual)
18. Sections 1801, et seq. of title 50, United States Code (also known as “The Foreign Intelligence Surveillance Act of 1978, as amended”)
19. Intelligence Community Directive 710, “Classification and Control Markings System,” September 11, 2009
20. The US Government Manual
    - http://www.usgovernmentmanual.gov
21. ISA STIX™ Profile Report v1-1,
    - https://community.max.gov/download/attachments/699566316/ISA%20STIX%20Profile%20Report%20v1.docx?version=1&modificationDate=1395857509190&api=v2
22. ESSA Max.gov site
    - https://community.max.gov/pages/viewpage.action?pageId=695866673
23. Executive Order 13526, Classified National Security Information, December 29, 2009
24. Department of Homeland Security Management Directive Number 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information, January 6, 2005.
25. Intelligence Community Directive 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*
26. Intelligence Community Technical Specification XML Data Encoding Specifications for Information Security Markings, Version 2014-DEC
    - http://purl.org/ic/standards/ISM (Requires Intellink-U to access)
27. Controlled Vocabulary Enumeration Values for FAC (FAC-CVEnums), December 22, 2014
    - http://purl.org/ic/standards/ISM (Requires Intellink-U to access)
28. Executive Order 12333, United States Intelligence Activities
29. Controlled Vocabulary Enumeration Values for USAgency (USAgency-CVEnums), February 2, 2015
    - http://purl.org/ic/standards/ISM (Requires Intellink-U to access)
30. Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
    - https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promotingprivate-sector-cybersecurity-information-sharing
31. Geopolitical Entities, Names, and Codes (GENC) Standard Edition 1
    - http://www.fgdc.gov/standards/organization/FGDC-SWG/meetings/2013-01-30_SWGmaterials/GENC/at_download/file
32. ISO 3166-1 International Organization for Standardization (ISO). Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. ISO 3166-1:2006
    - http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719
33. Intelligence Community Technical Specification Access Control Encoding Specification for Information Security Markings, Version 2014-DEC
    - http://purl.org/ic/standards/ISM (Requires Intellink-U to access)

34. ISO 8601 International Organization for Standardization (ISO) Date and time format http://www.iso.org/iso/iso8601
35. Presidential Policy Directive-21 “Critical Infrastructure Security and Resilience”
    - http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directivecritical-infrastructure-security-and-resil
36. Cybersecurity Information Sharing Act of 2015
    - https://www.congress.gov/bill/114th-congress/senate-bill/754

Acronyms

ABAC	Attribute-Based Access Control
AICP	Authorized IC Person
AOI	Areas of Interest
AOR	Areas of Responsibility
ATO	Authority to Operate
CA	Certification Agent
CCOI	Cross-organizational Communities of Interest
CIKR	Critical Infrastructure/Key Resources
CNCI-5	Comprehensive National Cybersecurity Initiative Five
CNWDI	Critical Nuclear Weapons Design Information
CNWDI	Critical Nuclear Weapons Design Information
COI	Community of Interest
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority
DC3	Defense Cyber Crime Center
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DN	Distinguished Name
DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
ECS	Enhanced Cybersecurity Services
EFE	Enduring Functional Exchanges
EIAS	DoD Enterprise Identity Attribute Service
EO	Executive Order
ESSA	Enhance Shared Situational Awareness
FBI	Federal Bureau of Investigation
FGI	Foreign Government Information
FICAM	Federal Identity, Credential, and Access Management
FVEY	Five Eyes

GFIPM	DoJ Global Federated Identity and Privilege Management
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
IC ITE	Intelligence Community Information Technology Enterprise
IC-EDH	Intelligence Community Enterprise Data Header
IC-SCC	Intelligence Community Security Coordination Center
IOA	Integrated Operational Action
ISA	Information Sharing Architecture
ISO	International Organization for Standardization
IT	Information Technology
JOC	Joint Operations Center
LOA	Levels of Assurance
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
NSPD	National Security Presidential Directive
NTOC	NSA/CSS Threat Operations Center
OCA	Original Classification Authority
PBAC	Policy-Based Access Control
PCII	Protected Critical Infrastructure Information
PKI	Public Key Infrastructure
PII	Personally Identifiable Information
POC	Point of Contact
PPD	Presidential Policy Directive
RAdAC	Risk-Adaptable Access Control
RBAC	Role-Based Access Control
S	Secret
SAP	Special Access Programs
SAR	Special Access Restrictions
SCI	Sensitive Compartmented Information
SCI	Sensitive Compartmented Information
SD-EDH	Smart Data – Enterprise Data Header
SSA	Shared Situational Awareness
STIX	Structured Threat Information eXpression
TLP	Traffic Light Protocol

TR	Technology Requirement
TS	Top Secret
U	Unclassified
UAAS	Unified Authorization and Attribute Service
UIAS	Unified Identity Attribute Set
USG	United States Government

Glossary

Attribute Provider or Store	A trusted authoritative source that provides the attributes associated with a person or NPE.
Authentication	The process of verifying the identity claimed by or assumed of an entity (i.e., check that I am who I say I am).
Authorization	Access privileges granted to an authenticated user, program or process, or the act of granting those privileges (i.e., check what I am allowed to see).
Entity (or Subject) Attribute	Characteristics about the person or non-person entity (NPE) who is requesting access that is used to make authorization decisions (e.g., clearance level).
Environmental Attribute	Attributes about the current environment at the time of the transaction itself (e.g., time of day, threat level, and physical location of entity requesting access).
FICAM Attribute Registry	Central location for interested parties to identify the types of attributes that can be leveraged across the Federal Government and external partners. The FICAM Attribute Registry specifies attribute names, syntax, and semantics. • Note: The FICAM Attribute Registry is a governance process for maintaining the definitions of attributes only. It is not a common storage for attributes associated with specific people.
Ignored Entity Attribute	The attribute is explicitly not used in making access decisions at that classification level.
ISA STIX Profiles	A set of business rules specific to the ISA community to guide the implementation of STIX (Reference 11) to ensure interoperability.
Non-Person Entity (NPE)	[A]n entity with a digital identity that acts in cyberspace, but is not a human actor. This can include analytics or automated decision engines.
Optional Entity Attribute	Someone seeking access to a resource may provide the attribute, but that it can also be left empty. Therefore, the access rules may require that information for use in the decision. If the attribute is considered necessary to gain access to a resource but is not provided, then access is denied.
Policy	Those documents that outline the general principles and acceptable procedures of a governmental organization. Individual components of those documents are also known as policies.
Policy Rules	Rules that specify how to use the above attributes (along with other things) to render an access decision.
Required Entity Attribute	Anyone seeking access to a resource must provide the attribute. Therefore, the access rules can expect to have that information for use in the decision. “Required” *does not* mean that the attribute must be used in making the access decision.

Resource Attribute	Information about the resource being requested (e.g., classification of data). Resources include data, applications, and services.

Appendix A: List of Organizations

The following list represents the list of organization values that are permitted for the resource attribute ORG and user attribute Duty Organization and used for making access control decisions for ISA exchanges. The list will also be used for the resource attribute CUST.

The values were derived based on the schema in Table A1. The second level of the Federal Government organization value is based on the US Government Manual (Reference 20) with some changes made based on ISA Use Cases. The third level organizational value will be controlled by the second level organization. However, until those values are maintained under organizational governance, the following list will be the required values for CUST and ORG. It is recommended that the schema in Table A1 be used if additional values for the attribute ORIG are needed.

This list allows the inclusion of the Cyber Centers and separation into hierarchical categories. Access control capabilities shall understand the hierarchical nature of the ORG attribute. Access will be granted to resources marked with a higher level ORG to entities that include the high level DUTYORG and lower level organizations. For example, for a resource marked ORG:USA.DOD, access shall be granted to users with the DUTYORG:USA.DOD.DC3. The reverse is not true. Resources marked with ORG:USA.DOD.DC3 will only be allowed access to entities with DUTYORG:USA.DOD.DC3 or lower.

Federal Government Organizations

USA.CIA	Central Intelligence Agency
USA.CTIIC	Cyber Threat Intelligence Integration Center
USA.DIA	Defense Intelligence Agency
USA.DHS	Department of Homeland Security
USA.DHS.CBP	US Customs and Border Protection
USA.DHS.ICE	US Immigration and Customs Enforcement
USA.DHS.NCCIC	National Cybersecurity and Communications Integration Center
USA.DHS.NCSC	National Cyber Security Center
USA.DHS.TSA	Transportation Security Administration
USA.DHS.USCG	US Coast Guard
USA.DHS.US-CERT	United States Computer Emergency Readiness Team
USA.DHS.USSS	US Secret Service
USA.DISA	Defense Information Systems Agency
USA.DNI	Office of the Director of National Intelligence
USA.DNI.IC-SCC	Intelligence Community – Security Coordination Center
USA.DOC	Department of Commerce
USA.DOC.NIST	National Institute of Standards and Technology
USA.DOD	Department of Defense
USA.DOD.AFCYBER	US Air Force Cyber Command
USA.DOD.ARCYBER	US Army Cyber Command

USA.DOD.C10F	US Navy Fleet Cyber Command
USA.DOD.DC3	Defense Cyber Crime Center
USA.DOD.MARFORCYBER	Marine Corps Cyberspace Command
USA.DOD.USA	US Army
USA.DOD.USAF	US Air Force
USA.DOD.USCYBERCOM	US Cyber Command
USA.DOD.USCYBERCOM-JOC	US Cyber Command Joint Operations Center
USA.DOD.USMC	US Marine Corps
USA.DOD.USN	US Navy
USA.DOD.USSTRATCOM	US Strategic Command
USA.DOE	Department of Energy
USA.DOJ	Department of Justice
USA.DOJ.DEA	Drug Enforcement Agency
USA.DOJ.FBI	Federal Bureau of Investigation
USA.DOS	Department of State
USA.DOT	Department of Transportation
USA.DOT.FAA	Federal Aviation Administration
USA.ED	Department of Education
USA.EOP	Executive Office of the President
USA.GSA	General Services Administration
USA.HHS	Department of Health and Human Services
USA.HUD	Department of Housing and Urban Development
USA.NASA	National Aeronautics and Space Administration
USA.NCIJTF	National Cyber Investigative Joint Task Force
USA.NGA	National Geospatial-Intelligence Agency
USA.NRO	National Reconnaissance Office
USA.NSA	National Security Agency
USA.NSA.NTOC	National Security Agency/Central Security Service Threat Operations Center
USA.SSA	Social Security Administration
USA.TREAS	Department of Treasury
USA.USDA	Department of Agriculture
USA.USG	US Government (Used to represent all organizations in this Federal Government Organizations list. For use as ORG token only; not with CUST, ORIG, or user entity attributes.)

SLTT (State, Local, Tribal, Territorial) Government Organizations

The only token for the CUST for a State, Tribal, or Territorial organization will be the alpha-2 code indicating the specific organization:

USA.XX	Individual state, territorial, or tribal government where XX=two letter postal abbreviations

The following organizational groupings can be used for dissemination purposes with the FurtherSharing attribute and Originator attribute:

USA.SLTT	All State, Local, Tribal and Territorial government civilian employee

USA.STA All State Government civilian employee
USA.TER US Territorial government civilian employee
USA.TRB Tribal government (within the US) civilian employee
USA.SLTT.FUSION State and Major Urban Area Fusion Centers

Non-governmental Organizations

There are currently no non-governmental organizations that will be custodians (CUST) of ISA data. The following non-government organizational groupings are FurtherSharing and Originator values. If additional non-governmental values for the attribute ORIG are needed the schema in Table A1 should be used.

CDC Cleared Defense Contractors
CIKR Critical Infrastructure and Key Resources
DIB Defense Industrial Base
FIN Financial Industry
ISAC Information Sharing and Analysis Centers
NONFED Non-Federal Entities
PRIVATESECTOR Private Sector Entities

Table A1: ORG value schema

Corresponding DNS Domain	Organization Type	Country	Gov Level	Tag category	Level 1 Tag Component	Level 2 Tag Component	Level 3 Tag Component	Example
.gov, .mil	Governmental/ Military Organization	USA	National-level	(all USG less congressional)	USA	USG	[n/a]	ORG:USA.USG
				(individual orgs)		<US Agencies>	[suborg lists controlled by each dept]	ORG:USA.DHS.ICE
			SLTTlevel	(all State/Tribe/Territory)		SLTT	[Common organizationsacross SLTT such as fusion centers]	ORG:USA.SLTT
				(individual STA entities)		<STA list>	[Local lists controlled by each S/T/T]	ORG:USA.AZ.DPS
		(other countries)			<alpha-3 country codes>	[lists controlled by each country]		ORG:GBR.GCHQ
.int	International Organization				INT	<DNS intl org list>		ORG:INT.NATO
.org (.ngo)	Non-Governmental Organization				[n/a]			
.org	Non-Profit Organization				NPO	[.org name?]		ORG:NPO.MITRE
	Religious Organization				[n/a]			

	(Other)		[n/a]			
.edu	Higher Education Organization		EDU	[.edu name]		ORG:EDU.CMU
.com, .net, .biz	NASDAQ-traded corporation		COM	<NASDAQ company list>		ORG:COM.LMT
	(Other)			[.com/.net/.biz name]		ORG:COM.ciphercloud

B: Summary of Derived ISA Requirements

TR-18	"*All data objects exposed for sharing shall have the Information Control metadata listed in Table 12: Summary of ISA Resource Attributes.* " (Reference 3)
TR-18.1	Upon sharing via ISA capabilities, ISA data producers shall limit resource access attributes to those listed in the ISA ACS.
TR-18.2	ISA access control mechanisms shall make access control decisions using only ISA Resource Attributes
TR-18.3	Data producers shall provide a unique resource identifier for each shared resource.
TR-18.4	Data producers shall provide a resource creation date and time for each shared resource.
TR-18.5	Data producers shall provide a custodian for each shared resource.
TR-18.6	Data producers shall provide the classification for each shared resource.
TR-18.8	If a resource has sensitivity or shareability restrictions, then Formal Determination shall not include Public Releasable.
TR-31	*"The access control business rules shall protect each ISA Participant's shared resources to the degree required by that Participant's information control tags." (Reference 3)*
TR-31.1	ISA information consumers shall maintain the data producer's access control constraints.
TR-83	*"The access control mechanism shall authenticate and authorize the consumer."* (Reference 3)
TR-83.1	The access control mechanism shall only grant access to consumers that hold an equivalent or higher clearance than the classification of the resource.
TR-83.2	If a resource has special control restrictions, then the access control mechanism shall only grant access to consumers that hold all of the corresponding special control permissions.
TR-83.3	If a resource has Sensitivity restrictions, then the access control mechanism shall only grant access to consumers that hold all of the corresponding entity attributes as defined by the Access Group policies.
TR-83.4	If a resource has Country Disclosure restrictions, then the access control mechanism shall only grant access to consumers that are affiliated with at least one of the countries identified.
TR-83.5	If a resource has Organizational Dissemination restrictions, then the access control mechanism shall only grant access to consumers that are affiliated with at least one of the organizations identified.
TR-83.6	If a resource has Entity Dissemination restrictions, then the access control mechanism shall only grant access to consumers with an Entity Type that corresponds to one of the Entity values identified.
TR-83.7	If a resource has Shareability restrictions, then the access control mechanism shall only grant access to consumers that are affiliated with at least one of the Access Groups identified.
TR-83.8	If a resource has LAC restrictions, then the access control mechanism shall only grant access to consumers that hold all of the corresponding LAC permissions.
TR-20	*"All users and non-person entities (NPEs) shall have the identification and authorization metadata listed in Table 13: Summary of ISA Entity Attributes"* (Reference 3)

Appendix

TR-20.2	ISA access control mechanisms shall make access control decisions using only the entity attributes defined in the ISA ACS.
TR-20.3	Each person entity and non-person entity (NPE) shall have an AdminOrganization attribute accessible by ISA access control mechanisms.
TR-20.4	Each non-person entity (NPE) shall have an Authority to Operate (ATO) Status attribute accessible by ISA access control mechanisms.
TR-20.5	Each person entity shall have an Authorized IC Person (AICP) Status attribute at the TS network level accessible by ISA access control mechanisms.
TR-20.6	Each person entity and non-person entity (NPE) shall have a Clearance attribute on classified network levels accessible by ISA access control mechanisms.
TR-20.7	Each person entity and non-person entity (NPE) shall have a Country of Affiliation attribute accessible by ISA access control mechanisms.
TR-20.8	Each person entity and non-person entity (NPE) shall have a Digital Identifier accessible by ISA access control mechanisms.
TR-20.9	Each person entity and non-person entity (NPE) shall have a Duty Organization attribute accessible by ISA access control mechanisms.
TR-20.10	Each person entity and non-person entity (NPE) shall have an Entity Type attribute accessible by ISA access control mechanisms.
TR-20.11	Each person entity and non-person entity (NPE) shall have a Fine Access Controls attribute at the TS network level accessible by ISA access control mechanisms.
TR-20.12	Each person entity and non-person entity (NPE) shall have an Is IC Member attribute at the TS network level accessible by ISA access control mechanisms.
TR-20.13	Each non-person entity (NPE) shall have a Life Cycle Status attribute accessible by ISA access control mechanisms.

C: Deltas between ISA ACS Entity Attributes and UIAS/EIAS/GFIPM

The ISA Access Control Specification Entity Attributes are based on the entity attributes of the UIAS (Reference 6). In addition, the DoD EIAS (Reference 7) and the DOJ GFIPM (Reference 8) attributes were evaluated for ease of mapping between the different specifications (Table C-1). An indication in the table that the attributes are aligned indicates that the names, intended usage, and values are the same.

Table C-1: Entity Attribute Mappings

ISA Entity Attribute Name	UIAS	EIAS	GFIPM
Admin Organization	Admin Organization (aligned)	ADM_ORG_CD	Employer Name or Owner Agency Name
Authority Category	Authority Category (aligned)		
Access Groups	(not aligned)		
ATO Status	ATO Status (aligned)	N/A	
Authorized IC Person	AICP (aligned)		
Clearance	Clearance (not aligned)	JPAS_ACS_CD, JPAS_ELIG_CD	Clearance Code
Country of Affiliation	Country Of Affiliation (not aligned)	CTZP_CTRY_CD	Citizenship Code
Digital Identifier	Digital Identifier (aligned)	DOD_EDI_PN_ID	Electronic Identity Id
Duty Organization	Duty Organization (not aligned)	DUTY_DOD_OCC_CD	Assignment Agency Name
Entity Type	Entity Type (aligned)	DOD_ASSOC_CD	Organization General Category Code
Fine Access Controls	Fine Access Controls (aligned)		
Is IC Member	Is IC Member (aligned)		
Life Cycle Status	Life Cycle Status (aligned)	N/A	

The goal was to make as few modifications to the UIAS Version 3 as possible. However, modifications were made, mainly to the allowable values for the attributes as specified in Section 3, to address the needs of the cybersecurity community beyond the Intelligence Community and to align with the SD-EDH Resource Attributes. Significant differences include:

- The UIAS Version 3 includes several new attributes which should be considered for future addition to the ACS Entity Attributes, including:
    - ○ Entity Security Mark to specify the shareability of the entity information beyond the network on which it is hosted ○ IC Network to specify the network to which the NPE is connected

Appendix

- UIAS contains attributes Region, Role, and Topic which were not needed based on the ESSA Information Sharing Participant Use Cases and were, therefore, not included in the ACS.
- The ACS Access Groups provides a broader set of groups to which a person can be assigned than the UIAS Authority Category. For the Authority Category, the allowable values are included in the Logical Authority Categories in the NSA Master Registry and in future versions of UIAS will be encoded in an XML CVE Encoding Specification for Authority Categories. The ACS Access Groups includes the broader set to support the assignment of Shareability and Sensitivity permissions. The Entity Standards Tiger Team (ESTT), responsible for updates to the UIAS, is considering changes to UIAS to incorporate some of the concepts related to groups but, at this time, these attributes are not aligned.
- The allowable values for the Clearance attribute are more limited in this ACS than specified in UIAS. The ACS limits the number of values to a single value and to the US government marking system clearances. This ACS does not support the use of interim clearances, Department of Energy clearances, or Foreign Government clearances.
- For Country of Affiliation, the ACS specifies the GENC Country Codes (Reference 31) while the UIAS specifies ISO 3166-1 (Reference 32). The GENC Standard Edition 1.0 is the US Government implementation of ISO 3166-1 that conforms to US Board on Geographic Names and US Government recognition policy.
- For Digital Identifier, the ACS and UIAS are in alignment. However, future review should consider the use of FASCN or a UUID as a key to retrieve entity attributes in lieu of the DN in order to prevent any concerns regarding the DN and privacy and to align more closely with FICAM specification (Reference 5).
- For Duty Organization, the ACS specifies the allowable values in Appendix A which differs from the UIAS allowable values from the Controlled Vocabulary Enumeration for USAgency (Reference 29). ESSA Information Sharing Participants agreed that the US Agency acronym list did not provide sufficient granularity or a hierarchy to support ISA Use Cases.

As ISA capabilities are implemented and UIAS continues to change to meet the needs of the Intelligence Community, ESSA should consider aligning the ACS Entity Attributes completely with UIAS and work with the IC change process to make modifications to support ESSA's requirements.

D: Deltas between ISA ACS Resource Attributes and IC Security Marking Encodings

The ISA Access Control Specification Resource Attributes are based on the Smart Data – Enterprise Data Header which differs from the Intelligence Community – Enterprise Data Header (Reference 9). Table Table D-1: Resource Attribute Mappings

Table D-1: Resource Attribute Mappings

ACS Resource Attributes (as documented in SD-EDH Cyber Profile) (Reference15)	IC-EDH Attribute	Differences and Justification

Identifier Example: isa:guide.19001.40af97be00bf-4648-9e70-296a6a8edab2	ICEDH-Identifier Example: guide://200001/40af97be00bf-4648-9e70-296a6a8edab2	This ACS specifies different format (not IC ID) because of incompatibility with marking STIX documents.
CreateDateTime (ISO 8601 extended with time zone)	ICEDH-DataItemCreateDateTime	Aligned
ResponsibleEntity Custodian Originator See notes related to Rights and Responsibilities of CUST and ORIG[10] Allowable values are specified in Appendix A of the ACS.	ICEDH-ResponsibleEntity Sub-elements: Country Organization Sub-organization	The ACS Responsible Entity is not aligned with the format or the XML CVE Encoding Specifications used for the ICEDH-ResponsibleEntity. ESSA uses a hierarchical organization listing included in Appendix A which precludes the need for the Country and SubOrganization subelements. ESSA requires the capability to specify the originator of the resource in the case that it is not the Custodian.

ACS Resource Attributes (as documented in SD-EDH Cyber Profile) (Reference15)	**IC-EDH Attribute**	**Differences and Justification**
AuthRef URN Example: urn:isa:authority:ABCDEF	ICEDH-AuthorizationReference Example: 3249	There is limited registry capability in support of ISA implementation. The SD-EDH and IC-EDH use different formats.

[10] Rights and responsibilities of Originator and Custodian ORIG: responsible to: check that they can share data; meet legislative obligations; ensure their own equities are protected; set mandatory and optional data handling requirements on custodian; liaise with CUST in incident handling; capture origin of data. CUST: responsible to: check that they are legally allowed to access data; check that they meet legislative obligations; respect and protect the equities of the ORIG; respect data handling obligations; carry out incident procedures.

Appendix

No mapping	ICEDH-OwnerProducer Example: USA	IC specifies which organization is the OwnerProducer of the security marking system. ISA Participants agreed to use the ACS markings limiting the security markings to the US marking system.
PolicyRef		The ACS permits the use of a policy by reference.
Policy		See Policy Substitution Group Table D-2.
Classification Values: TS, S, C, U	ICEDH-Classification (ism)	ISA uses only the US classification system and does not allow Restricted (R) data.
SCI Controls Values: As listed in the NSA Master Registry	ICEDH-SCIcontrols (ism)	Aligned.
Logical Authority Category (LAC) Example: LAC:EO12333_X	ICEDH-LAC	This attribute is only specified on a TS network. Aligned.
Shareability (SHAR) Values: NCC, EM, LE, IC,	ICEDH-AccessAuthorizationList (ntk)	It is possible to implement some concepts of shareability using the IC ntk construct but the specifications are not aligned related to Shareability markings.
Sensitivity (SENS) Example: SENS:Test_COI, PCII, LES, INT, PII, PR, TEI	ICEDH-COI (ntk) Some values map to disseminationControls Not in IC are: PCII, INT, PII, TEI	It is possible to implement some concepts of sensitivity using the IC ntk construct but the specifications are not aligned related to sensitivity. FOUO is included as an ism:disseminationControls.

ACS Resource Attributes (as documented in SD-EDH Cyber Profile) (Reference15)	IC-EDH Attribute	Differences and Justification
Caveat (CVT) Values: FISA, POSSIBLEPII	ism:disseminationControl FISA included as a disseminationControl value but not used for access control	The ISA values are not used for access controls and neither is the FISA caveat in the IC. Although not well aligned, they do not conflict.
Formal Determination (FD) Values: PUBREL, NF, AIS, PIINECESSARY-TO-UNDERSTAND-THREAT, PII-NOT-PRESENT, FOUO	ICEDH-disseminationControls (ism) Some of the DissemControls map to SENSGRP and CUI DissemControl= NF maps to CTRY=USA ism:disseminationControls The following values are not used the SD-EDH Cyber profile: RS, OC, OC-USG, IMC, RELIDO, EYES, DSEN, DISPLAYONLY, LIMDIS, EXDIS, NODIS, SBU, SBU-NF, LES-NF, SSI, NNPI, ACCM The following values are assigned differently: RS – not used in SD-EDH Cyber profile FOUO – assigned as Formal Determination NF – considered a Formal Determination PR – assigned as a Sensitivity (PROPIN) REL – not used – can be specified as CTRY restriction FISA – assigned as Caveat LES – assigned as Sensitivity	The ACS indicates that the FD values are not used for Access Control decisions. The ACS links NF to limitations placed using CTRY. The ACS uses AccessPrivilege to limit further actions instead of OC. The ACS uses PUBREL in coordination with a PublicRelease Policy. There are also differences in ORG listings. ICEDH used USAgency CVE. ACS uses Appendix A List. The ACS has added a value of AIS to the FD attribute in support of the DHS Automated Indicator Sharing Initiative.
Country (CTRY) (restriction)	ICEDH-releaseableTo (ism)	The ACS uses an alternative encoding to the IC ISM, e.g. “Country” element instead of IC ISM’s “Rel To” or “DisplayOnly” attributes. The “Country” and “Rel To” constructs

ACS Resource Attributes (as documented in SD-EDH Cyber Profile) (Reference15)	IC-EDH Attribute	Differences and Justification

Organization (ORG) (restriction)	(ntk) only US Federal organizations	The allowed values for ORG do not align with the IC's definition of USAgency. The USAgency CVE does not support the ISA requirements related to restriction to sub organizations.
Entity (ENTITY) (restriction)	ICEDH-Entity	Aligned
	ICEDH-Issue (aka Topic) ICEDH-SubRegion	SD-EDH Cyber does not include Issues, Topics or Subregions.
	ICEDH-Notice	SD-EDH Cyber does not include Notices.

Appendix E: Access Control Rule Set Example

Access Control Policies are rules that specify how to use the ACS attributes to render an access decision. Section 4 of the ACS provided examples of applying policies to the ISA Entity and Resource Attributes. Table 4-1-1 defined the relationships between ISA Entity and Resource Attributes. This appendix includes pseudocode examples of how those policies might be implemented.

Objects: Resource, Network, User

CHECK RESOURCE CLASSIFICATION

```
// Assumption: Resource must have a classification
IF (Resource Classification = NULL)
      RETURN CLASSIFICATION ERROR

// Assumption: Only allowable values are TS, S, C, & U
      and TS>S>C>U
IF (Resource Classification > Network Classification)
  RETURN CLASSIFICATION ERROR

// Assumptions: See above, and a User 'R' Clearance is ignored
IF (Resource Classification > User Clearance)
  RETURN 'ACCESS DENIED'
```

CHECK SCI CONTROLS

```
// Assumption: A resource is mismarked if it has an SCI control
and is marked UNCLASSIFIED
IF (Resource SCI Controls != NULL ) AND (Network Classification = U)
RETURN CLASSIFICATION ERROR

IF (Resource SCI Controls != NULL)
      FOR EACH Resource SCI Control
          IF Resource SCI Control NOT IN Allowable SCI Controls List
RETURN VALUE ERROR

IF (Resource SCI Controls != NULL ) AND (Network Classification > U)
      IF (User Fine Access Control List = NULL)
            RETURN 'ACCESS DENIED'
       FOR EACH Resource SCI Control
          IF Resource SCI Control NOT IN User Fine Access Control List
RETURN 'ACCESS DENIED'
```

CHECK AUTHORITY CATEGORY

```
IF (Resource Authority Category != NULL)
```

```
        FOR EACH Resource Authority Category
            IF Authority Category NOT IN Allowable Resource Authority Category List
RETURN VALUE ERROR
        IF (User Authority Category List = NULL)
                RETURN 'ACCESS DENIED'
        FOR EACH Resource Authority Category
                IF Resource Authority Category NOT IN User Authority Category List
RETURN 'ACCESS DENIED'
```

CHECK SHAREABILITY

// Assumption: Since this is an OR, there is no need to check that each value of SHAR is in the allowable values list. If this assumption is correct, it may still be useful to make sure at least one value is acceptable, which this pseudo-code does not do.

```
    IF (Resource Shareability != NULL )
        IF (User Access Group List = NULL)
                RETURN 'ACCESS DENIED'
         FOR EACH Resource Shareability
            IF Resource Shareability IN User Access Group List
                SET Passed = TRUE
                BREAK
         IF (Passed != TRUE)
            RETURN 'ACCESS DENIED'
```

CHECK SENSITIVITY

```
    IF (Resource Sensitivity != NULL)
        FOR EACH Resource Sensitivity
            IF Sensitivity NOT IN Allowable Sensitivity List
                RETURN VALUE ERROR

       FOR EACH Resource SENS
                IF (User Access Group List = NULL)
                RETURN 'ACCESS DENIED'

                RETURN 'ACCESS DENIED'
```

CHECK COUNTRY

// Assumption: Since this is an OR, there is no need to check that each value of Country is in the allowable values list. If this assumption is correct, it may still be useful to make sure at least one value is acceptable, which this pseudo-code does not do.

```
    IF (Resource Country != NULL )
        IF (User Country of Affiliation  = NULL)
                RETURN 'ACCESS DENIED'
         FOR EACH Resource Country
            IF Resource Country IN User Country of Affiliation
```

```
            SET Passed = TRUE
            BREAK
      IF (Passed != TRUE)
         RETURN 'ACCESS DENIED'
```

CHECK ORGANIZATION

// Assumption: User only has 1 duty organization
// Assumption: Since this is an OR, there is no need to check that each value of Organization is in the allowable values list. If this assumption is correct, it may still be useful to make sure at least one value is acceptable, which this pseudo-code does not do.

```
   IF (Resource Organization != NULL )
      IF (User Duty Organization = NULL)
            RETURN 'ACCESS DENIED'
      FOR EACH Resource Organization
         IF Resource Organization = User Duty Organization
            SET Passed = TRUE
            BREAK


      IF (Passed != TRUE)
         RETURN 'ACCESS DENIED'
```

CHECK ENTITY

// Assumption: User only has 1 Entity Type
// Assumption: Since this is an OR, there is no need to check that each value of Entity is in the allowable values list. If this assumption is correct, it may still be useful to make sure at least one value is acceptable, which this pseudo-code does not do.

```
   IF (Resource Entity != NULL )
      IF (User Entity Type = NULL)
            RETURN 'ACCESS DENIED'
        FOR EACH Resource Entity
           IF Resource Entity = User Entity Type
            SET Passed = TRUE
            BREAK OUT OF FOR EACH LOOP
        IF (Passed != TRUE)
           RETURN 'ACCESS DENIED'
```

ALL CHECKS PASSED, SO GRANT ACCESS

This page intentionally left blank

Approved by: _____ Date: 2/19/2016
Mary Ann Anderson, NSA
Enhance Shared Situational Awareness Lead

Approved by: _____ Date: 2/19/2016
Charles Bulkley, FBI
Enhance Shared Situational Awareness Lead

Approved by: _____ Date: 2/19/2016
Antonio "T" Scurlock, DHS
Enhance Shared Situational Awareness Lead