



Intelligence Community Technical Specification

Access Control Encoding Specification for Information Security Markings

Version 2021-NOV

December 1, 2022

Distribution Notice:

This document has been approved for Public Release and is available for use without restriction.

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Enterprise Need	1
1.4 - Conventions	2
1.4.1 - XML Namespaces	2
1.5 - Dependencies	3
1.5.1 - Specification Dependencies	3
1.5.2 - Inverse Dependencies	4
Chapter 2 - Development Guidance	5
2.1 - Understanding Access Control	5
2.2 - Additional Guidance	5
2.2.1 - The URI	5
2.2.2 - Basic Usage	5
2.2.3 - Required Conditions for Access	5
2.2.4 - Non-USA Country Affiliation Access	5
2.2.5 - Handling Prior CVE Versions	6
2.3 - Need-To-Know and Access Control	6
2.3.1 - Guidance for systems processing data containing NTK metadata	7
2.4 - Potential Unauthorized Disclosure Data Spill Procedures	8
Chapter 3 - Constraints	9
3.1 - Valid ISM Marked Data	9
Chapter 4 - Conformance Validation	10
4.1 - Schema Validation	10
4.2 - Business Rule Validation	10
Chapter 5 - Access Control (AC-3)	11
5.1 - Classification	11
5.1.1 - Classification	11
5.1.2 - JOINT Classification	12
5.1.3 - NATO Classification	14
5.1.4 - NATO NAC Classification	17
5.2 - SCI Controls	21
5.3 - Special Access Programs	21
5.4 - AEA Controls	24
5.4.1 - Restricted Data (RD)	25
5.4.2 - Critical Nuclear Weapon Design Information (CNWDI)	25
5.4.3 - RD-SIGMA 14	25
5.4.4 - RD-SIGMA 15	26
5.4.5 - RD-SIGMA 18	26
5.4.6 - RD-SIGMA 20	27
5.4.7 - Formerly Restricted Data (FRD)	27
5.4.8 - FRD-SIGMA 14	27
5.4.9 - FRD-SIGMA 15	28
5.4.10 - FRD-SIGMA 18	28
5.4.11 - FRD-SIGMA 20	29
5.4.12 - DoD Unclassified Controlled Nuclear Information (DCNI)	29

5.4.13 - DoE Unclassified Controlled Nuclear Information (UCNI)	31
5.4.14 - Transclassified Foreign Nuclear Information (TFNI)	32
5.5 - Foreign Government Information Markings	32
5.5.1 - FGI Protected	32
5.5.2 - FGI Open NATO	33
5.6 - Dissemination Controls	35
5.6.1 - Risk Sensitive (RS)	35
5.6.2 - For Official Use Only (FOUO)	35
5.6.3 - Originator Controlled (OC)	36
5.6.4 - Originator Controlled US Government (OC-USGOV)	37
5.6.5 - Controlled Imagery (IMC)	37
5.6.6 - Not Releasable To Foreign Nationals (NF)	38
5.6.7 - Caution-Proprietary Information Involved (PR)	39
5.6.8 - Authorized For Release To (REL)	39
5.6.9 - Releasable By Information Disclosure Official (RELIDO)	40
5.6.10 - Eyes Only (EYES)	41
5.6.11 - DEA Sensitive (DSEN)	42
5.6.12 - Raw Foreign Intelligence Surveillance Act (RAWFISA)	43
5.6.13 - Foreign Intelligence Surveillance Act (FISA)	43
5.6.14 - Authorized For Display But Not Release To (DISPLAYONLY)	44
5.6.15 - EXEMPT FROM ICD-501 DISCOVERY	47
5.7 - Non-IC Dissemination Controls	47
5.7.1 - Limited Distribution (LIMDIS)	47
5.7.2 - Exclusive Distribution (EXDIS)	48
5.7.3 - No Distribution (NODIS)	48
5.7.4 - Sensitive But Unclassified (SBU)	49
5.7.5 - Sensitive But Unclassified NOFORN (SBU-NF)	50
5.7.6 - Law Enforcement Sensitive (LES)	50
5.7.7 - Law Enforcement Sensitive NOFORN (LES-NF)	51
5.7.8 - Sensitive Security Information (SSI)	51
5.7.9 - Naval Nuclear Propulsion Information (NNPI)	53
5.7.10 - Alternate Compensatory Control Measure (ACCM)	53
5.8 - NATO Controls	53
5.8.1 - ATOMAL	54
5.8.2 - BALK	54
5.8.3 - BOHEMIA	54
5.9 - Need-To-Know Access Control	55
5.9.1 - Enterprise Role	56
5.9.2 - Exclusive Distribution	56
5.9.3 - Intelligence Community Only	57
5.9.4 - License	58
5.9.5 - Mission Need	58
5.9.6 - No Distribution	59
5.9.7 - Originator Controlled	60
5.9.8 - Permissive	61
5.9.9 - Proprietary Information for All US Government Employees	62
5.9.10 - Proprietary Information for Specified Members Only	63
5.9.11 - Custom Profiles for PROPIN	64
5.9.12 - Restricted Authority Category	64

5.9.13 - Restrictive	65
5.10 - Access Control Specification Specific Mappings	66
Chapter 6 - Flow Control (AC-4)	67
6.1 - Introduction	67
6.2 - Certificate Authority	68
6.3 - Originating Network	69
6.4 - Flow Control Specification Specific Mappings	69
Appendix A - Feature Summary	70
A.1 - ISM.ACES Feature Comparison	70
A.1.1 - Features from V2019-MARr2019-JUN to V2021-NOV	70
A.1.2 - Features from 2018-AUG to V2019-MARr2019-JUN	71
A.1.3 - Features from 2016-DEC to 2018-AUG	71
A.1.4 - Features from 2014-DEC to 2016-DEC	71
A.1.5 - Features from V1 to 2014-DEC	72
A.1.5.1 - Features Partial and N/A from V1 to 2014-DEC	72
Appendix B - Change History	73
B.1 - V2021-NOV Change Summary	74
B.2 - V2020-OCT Change Summary	75
B.3 - V2019-SEP Change Summary	75
B.4 - V2019-MARr2019-JUN Change Summary	76
B.5 - V2019-MAR Change Summary	76
B.6 - V2018-NOV Change Summary	77
B.7 - V2018-AUG Change Summary	77
B.8 - V2018-APR Change Summary	78
B.9 - V2017-JUL Change Summary	78
B.10 - V2016-DEC Change Summary	79
B.11 - V2016-SEP Change Summary	79
B.12 - V2015-AUG Change Summary	80
B.13 - V2014-DEC Change Summary	81
B.14 - V2 Change Summary	82
Appendix C - Mapping ISM and UIAS Access & Flow	83
C.1 - Introduction	83
C.2 - Classification	83
C.2.1 - General Physical Rules	83
C.2.1.1 - Non-USA Country Affiliation Access	83
C.2.2 - Classification	84
C.2.3 - JOINT Classification	84
C.2.4 - NATO Classification	85
C.2.5 - NATO NAC Classification	86
C.3 - SCI Controls	87
C.4 - Special Access Programs	88
C.5 - AEA Controls	90
C.5.1 - Restricted Data (RD)	90
C.5.2 - Critical Nuclear Weapons Design Information (CNWDI)	90
C.5.3 - RD-SIGMA 14	90
C.5.4 - RD-SIGMA 15	91
C.5.5 - RD-SIGMA 18	91
C.5.6 - RD-SIGMA 20	92
C.5.7 - Formerly Restricted Data (FRD)	92

C.5.8 - FRD-SIGMA 14	93
C.5.9 - FRD-SIGMA 15	93
C.5.10 - FRD-SIGMA 18	94
C.5.11 - FRD-SIGMA 20	94
C.5.12 - DoD Unclassified Controlled Nuclear Information (DCNI)	95
C.5.13 - DoE Unclassified Controlled Nuclear Information (UCNI)	96
C.5.14 - Transclassified Foreign Nuclear Information (TFNI)	97
C.6 - Foreign Government Information Markings	97
C.6.1 - FGI Protected	97
C.6.2 - FGI Open NATO	98
C.7 - Dissemination Controls	98
C.7.1 - Risk Sensitive (RS)	98
C.7.2 - For Official Use Only (FOUO)	99
C.7.3 - Originator Controlled (OC)	100
C.7.4 - Originator Controlled US Government (OC-USGOV)	100
C.7.5 - Controlled Imagery (IMC)	101
C.7.6 - Not Releasable To Foreign Nationals (NF)	101
C.7.7 - Caution-Proprietary Information Involved (PR)	102
C.7.8 - Authorized For Release To (REL)	102
C.7.9 - Releasable By Information Disclosure Official (RELIDO)	103
C.7.10 - Eyes Only (EYES)	104
C.7.11 - DEA Sensitive (DSEN)	105
C.7.12 - RAWFISA	107
C.7.13 - Foreign Intelligence Surveillance Act (FISA)	108
C.7.14 - Authorized For Display But Not Release To (DISPLAYONLY)	108
C.7.15 - Exempt from ICD-501 Discovery	111
C.8 - Non-IC Dissemination Controls	111
C.8.1 - Limited Distribution (LIMDIS)	111
C.8.2 - Exclusive Distribution (EXDIS)	112
C.8.3 - No Distribution (NODIS)	113
C.8.4 - Sensitive But Unclassified (SBU)	114
C.8.5 - Sensitive But Unclassified NOFORN (SBU-NF)	114
C.8.6 - Law Enforcement Sensitive (LES)	115
C.8.7 - Law Enforcement Sensitive NOFORN (LES-NF)	116
C.8.8 - Sensitive Security Information (SSI)	116
C.8.9 - Naval Nuclear Propulsion Information (NNPI)	117
C.8.10 - Alternate Compensatory Control Measure (ACCM)	117
C.9 - NATO Controls	118
C.9.1 - ATOMAL	118
C.9.2 - BALK	118
C.9.3 - BOHEMIA	118
C.10 - Mapping Need-To-Know Access Profiles to UIAS	118
C.10.1 - Introduction	118
C.10.2 - Mapping EXDIS to UIAS	119
C.10.3 - Mapping ICO to UIAS	120
C.10.4 - Mapping LICENSE to UIAS	121
C.10.5 - Mapping MN to UIAS	121
C.10.6 - Mapping NODIS to UIAS	122
C.10.7 - Mapping ORCON to UIAS	125

C.10.8 - Mapping Permissive to UIAS	126
C.10.9 - Mapping PROPIN to UIAS	128
C.10.9.1 - All US Government Employee PROPIN to UIAS Mapping	128
C.10.9.2 - PROPIN for Specified Members to UIAS Mapping	130
C.10.10 - Mapping RAC to UIAS	132
C.10.11 - Mapping Restrictive to UIAS	132
Appendix D - Mapping ISM and UIAS Flow Control	134
D.1 - Introduction	134
D.2 - Certificate Authority	134
D.3 - Originating Network	136
Appendix E - Glossary	138
Appendix F - List of Abbreviations	140
Appendix G - Bibliography	143
Appendix H - Points of Contact	149
Appendix I - IC CIO Approval Memo	150

List of Figures

Figure 1 - Related Specifications	4
---	---

List of Tables

Table 1 - XML Namepaces	3
Table 2 - Direct Dependencies	3
Table 3 - Classification	11
Table 4 - JOINT Classification	13
Table 5 - NATO Classification	15
Table 6 - NATO NAC Classification	18
Table 7 - SCI Control Systems	21
Table 8 - Special Access Programs	23
Table 9 - RD	25
Table 10 - RD-CNWDI	25
Table 11 - RD-SG-14	26
Table 12 - RD-SG-15	26
Table 13 - RD-SG-18	26
Table 14 - RD-SG-20	27
Table 15 - FRD	27
Table 16 - FRD-SG-14	28
Table 17 - FRD-SG-15	28
Table 18 - FRD-SG-18	28
Table 19 - FRD-SG-20	29
Table 20 - DCNI	30
Table 21 - UCNI	31
Table 22 - TFNI	32
Table 23 - FGI Protected	33
Table 24 - FGI Open	33
Table 25 - RS	35
Table 26 - FOUO	36
Table 27 - OC-USGOV	37
Table 28 - IMC	38
Table 29 - NF	39
Table 30 - REL	40
Table 31 - RELIDO	41
Table 32 - EYES	42
Table 33 - DSEN	42
Table 34 - RAWFISA	43
Table 35 - FISA	44
Table 36 - DISPLAYONLY	46
Table 37 - EXEMPT FROM ICD501 DISCOVERY	47
Table 38 - LIMDIS	47
Table 39 - EXDIS	48
Table 40 - NODIS	48
Table 41 - SBU	49
Table 42 - SBU-NF	50
Table 43 - LES	50
Table 44 - LES-NF	51
Table 45 - SSI	52
Table 46 - NNPI	53

Table 47 - ACCM	53
Table 48 - ATOMAL	54
Table 49 - BALK	54
Table 50 - BOHEMIA	55
Table 51 - Need-To-Know Access Policies	55
Table 52 - Enterprise Role Access List	56
Table 53 - EXDIS Access List	57
Table 54 - Restriction to IC Members	58
Table 55 - LICENSE-NTK Access List	58
Table 56 - MN-NTK Access List	59
Table 57 - ND-NTK Access List	60
Table 58 - ORCON Access Control Mapping	61
Table 59 - Permissive Access Control Mapping	62
Table 60 - All US Government Employee PROPIN Access List	62
Table 61 - Group PROPIN Access List	64
Table 62 - RAC-NTK Access List	65
Table 63 - Restrictive Access Control Mapping	66
Table 64 - Flow Control Summary	68
Table 65 - Certificate Authority	68
Table 66 - Originating Network	69
Table 67 - Feature Summary Legend	70
Table 68 - ISM.ACES Feature Comparison V2019-MARr2019-JUN to V2021-NOV	70
Table 69 - ISM.ACES Feature Comparison 2018-AUG to V2019-MARr2019-JUN	71
Table 70 - ISM.ACES Feature Comparison 2016-DEC to 2018-AUG	71
Table 71 - ISM.ACES Feature Comparison 2014-DEC to 2016-DEC	71
Table 72 - ISM.ACES Feature Comparison V1 to 2014-DEC	72
Table 73 - ISM.ACES Feature Comparison V1 to 2014-DEC	72
Table 74 - DES Version Identifier History	73
Table 75 - V2021-NOV Change History	74
Table 76 - V2020-OCT Change History	75
Table 77 - V2019-SEP Change History	76
Table 78 - V2019-MARr2019-JUN Change History	76
Table 79 - V2019-MAR Change History	77
Table 80 - V2018-NOV Change History	77
Table 81 - V2018-AUG Change History	78
Table 82 - V2018-APR Change History	78
Table 83 - V2017-JUL Change History	79
Table 84 - Data Encoding Specification V2016-DEC Change Summary	79
Table 85 - Data Encoding Specification V2016-SEP Change Summary	80
Table 86 - Data Encoding Specification V2015-AUG Change Summary	80
Table 87 - Data Encoding Specification V2014-DEC Change Summary	81
Table 88 - Data Encoding Specification V2 Change Summary	82
Table 89 - US Classification	84
Table 90 - JOINT Classification	85
Table 91 - NATO Classification	86
Table 92 - NATO NAC Classification	86
Table 93 - SCI Controls	88
Table 94 - Special Access Programs	89
Table 95 - RD	90

Table 96 - RD-CNWDI	90
Table 97 - RD-SG-14	91
Table 98 - RD-SG-15	91
Table 99 - RD-SG-18	92
Table 100 - RD-SG-20	92
Table 101 - FRD	93
Table 102 - FRD-SG-14	93
Table 103 - FRD-SG-15	94
Table 104 - FRD-SG-18	94
Table 105 - FRD-SG-20	95
Table 106 - DCNI	95
Table 107 - UCNI	96
Table 108 - TFNI	97
Table 109 - FGI Protected	97
Table 110 - FGI Open	98
Table 111 - RS	99
Table 112 - FOUO	99
Table 113 - OC	100
Table 114 - OC-USGOV	101
Table 115 - IMC	101
Table 116 - NF	102
Table 117 - PR	102
Table 118 - REL	103
Table 119 - RELIDO	104
Table 120 - EYES	105
Table 121 - DSEN	106
Table 122 - RAWFISA	108
Table 123 - FISA	108
Table 124 - DISPLAYONLY	110
Table 125 - FISA	111
Table 126 - LIMDIS	111
Table 127 - EXDIS	113
Table 128 - NODIS	113
Table 129 - SBU	114
Table 130 - SBU-NF	115
Table 131 - LES	115
Table 132 - LES-NF	116
Table 133 - SSI	117
Table 134 - NNPI	117
Table 135 - ACCM	117
Table 136 - ATOMAL	118
Table 137 - BALK	118
Table 138 - BOHEMIA	118
Table 139 - EXDIS Access Control Mapping	120
Table 140 - Restriction to IC Members	121
Table 141 - LICENSE-NTK Access List	121
Table 142 - MN-NTK Access List	122
Table 143 - ND-NTK Access List	124
Table 144 - ORCON Access Control Mapping	126

Table 145 - Permissive Access Control Mapping	127
Table 146 - All US Government Employee PROPIN Access List	128
Table 147 - Group PROPIN Access List	131
Table 148 - RAC-NTK Access List	132
Table 149 - Restrictive Access Control Mapping	133
Table 150 - Certificate Authority	135
Table 151 - Originating Network	136

Chapter 1 - Introduction

1.1 - Purpose

This *Access Control Encoding Specification for Information Security Markings* (ISM.ACES) defines detailed implementation guidance for providing access to documents which have *XML Data Encoding Specification for Information Security Markings* (ISM.XML^[27]) markup in them. This Access Control Encoding Specification (ACES) defines the combinational logic between data and user/entity attributes. This logic is intended to be used in the decision process of access control decisions based on Extensible Markup Language (XML) elements and attributes that represent ISM.XML^[27] data concepts and the associated user attributes.

1.2 - Scope

The *Intelligence Community Technical Specification Framework* (IC-SF.XML^[13]) defines the basic conceptual structure and outlines the core philosophy of Intelligence Community (IC) technical specifications. For convenience, a copy of this framework is included in every package.

This specification profile is applicable to the IC and information produced by, stored, or shared within the IC. This ACES may have relevance outside the scope of intelligence; however, prior to applying outside of this defined scope, the ACES should be closely scrutinized and differences separately documented and assessed for applicability.

This specification profile only applies to data marked with ISM.XML^[27] that is:

- Classified or created on or after 28 June 2010

OR

- Originator Controlled (ORCON) information

Executive Order (E.O.) 13526, *Classified National Security Information* ^[4], 29 December 2009 modified access decision logic for non-ORCON data. The access decision logic for non-ORCON data classified prior to 28 June 2010, the effective date of E.O. 13526^[4], is not yet codified in this ACES. Refer to E.O. 13526^[4] for the access logic.

Section 4.1 i (3) of E.O. 13526^[4] states:

Documents created prior to the effective date of this order shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

1.3 - Enterprise Need

Information security markings vary depending on if the data is from the IC, Department of Defense (DoD), Department of Energy (DOE), or North Atlantic Treaty Organization (NATO). There is a clear need to be able to understand these markings and make automated access control decisions. The ISM.ACES builds upon existing policies and guidance to accomplish this need.

Both enterprise needs and requirements for this specification can be found in the following policies and implementation guidance:

- 200 Series:
 - Intelligence Community Directive (ICD) 208, *Write for Maximum Utility* ^[14]
 - ICD 209, *Tearline Production and Dissemination* ^[15]
 - Intelligence Community Policy Memorandum (ICPM) 2007-200-2, *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide* ^[22]
- 500 Series:
 - ICD 500, *Director Of National Intelligence Chief Information Officer* ^[16]
 - ICD 501, *Discovery and Dissemination or Retrieval of Information within the IC* ^[17]
 - Intelligence Community Program Guidance (ICPG) 500.2, *Attribute-based Authorization and Access Management* ^[19]
 - Intelligence Community Standard (ICS) 500-20, *IC Enterprise Standards Compliance* ^[23]
 - ICS 500-21, *Tagging of Intelligence and Intelligence-Related Information* ^[24]
- 700 Series:
 - ICD 710, *Classification and Control Markings System* ^[18]
 - ICPG 710.1, *Application of Dissemination Controls: Originator Control* ^[20]
 - ICPG 710.2, *Application of Dissemination Controls: Foreign Disclosure and Release Markings* ^[21]
- Memorandums:
 - IC CIO Memo - *Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness* ^[8]
- DoD Issuances:
 - Department of Defense Manual 5205.07, *Special Access Program (SAP) Security Manual: Marking* ^[3]
- Executive Orders:
 - Executive Order 13526 *Classified National Security Information* ^[4]
 - Executive Order 13556 *Controlled Unclassified Information* ^[6]
- Implementing Directives:
 - 32 CFR Parts 2001 and 2003 *Classified National Security Information; Final Rule* ^[29]
 - 32 CFR Part 2002 *Controlled Unclassified; Final Rule* ^[30]
 - 32 CFR Parts 2003 *The Interagency Security Classification Appeals Panel (ISCAP) Bylaws, Rules, and Appeal Procedures* ^[31]
 - 32 CFR Parts 2004 *National Industrial Security Program Directive No. 1* ^[32]
 - ISOO Marking Booklet 2018 *Marking Classified National Security Information, Rev. 4 2018* ^[33]

1.4 - Conventions

Certain technical and presentation conventions are used in the creation of the IC technical specifications to ensure readability and understanding. For details, please see the "Specification Conventions" chapter in the IC-SF.XML ^[13].

1.4.1 - XML Namespaces

Namespaces referenced in this document and the prefixes used to represent them are listed in the following table. The namespace prefix of any XML Qualified Name used in any example in this document should be interpreted using the information below.

Table 1 - XML Namespaces

Prefix	URI
ism	urn:us:gov:ic:ism
tetra	urn:us:gov:ic:taxonomy:catt:tetragraph

1.5 - Dependencies

Specifications often rely on other specifications, components or artifacts, either directly or indirectly. For specific definitions of dependency terminology used throughout this section, please see the “Dependency Definitions” chapter in the IC-SF.XML^[13].

1.5.1 - Specification Dependencies

This technical specification directly depends on the technical specifications, documentation, and implementations listed in [Table 2](#). The dependencies listed below are directly referenced in this specification (e.g., Schema, Schematron), and are normative or informative as indicated.

The subsequent figure, [Figure 1](#), is an informative graphical representation of all of the Intelligence Community Chief Information Officer (IC CIO) specifications related to this specification. The graphic depicts dependencies. However, the representations may not match an exact schema import tree or dependency diagram that an analysis of the Schema, Schematron or other documents would yield. For example, the graphic only shows a given specification once even though it may actually be imported by many specifications or be a direct dependency. All IC CIO specifications listed in [Table 2](#) will be shown in [Figure 1](#); however not all IC CIO specifications listed in [Figure 1](#) may appear in [Table 2](#). [Figure 1](#) is to aid users in gaining a general understanding of all dependencies whether direct or transitive.

Table 2 - Direct Dependencies

Name	Dependency Description
<i>XML Data Encoding Specification for Unified Identity Attribute Set</i> (UIAS.XML.V2021-NOV+ ^[37])	This ACES depends on the current version of UIAS.XML ^[37] .
<i>XML Data Encoding Specification for Information Security Marking Metadata</i> (ISM.XML.V2021-NOVr2022-NOV+ ^[27])	This specification depends on the LATEST technically sound, approved version of ISM.XML ^[27] . The minimum version was based on compliance with the authoritative source, which is ICD-710 ^[18] . Per ICD-710, all security markings MUST be updated within 365 days of a release of the Register and Manual. As of this release, the latest version of ISM.XML is 2021-NOVr2022-NOV which is based on the Register and Manual released in August, 2019.
<i>CVE Encoding Specification for US Agency Acronyms</i> (USAgency.CES.V2021-NOV+ ^[38])	This ACES depends on the current version of USAgency.CES ^[38] .

Name	Dependency Description
<i>CVE Encoding Specification for ISM Country Codes and Tetragraphs</i> (ISM.CES.V2022-NOV+ ^[28])	This specification depends on the LATEST technically sound, approved version of ISMCAT.CES ^[28] . At the time of this release, the latest version of ISMCAT.CES is 2022-NOV and MUST be used unless a later, technically sound, approved version of ISMCAT.CES has been released. The requirement to use the latest technically sound, approved version is based on authoritative source compliance ^[36] .
<i>Intelligence Community Specification Framework</i> (IC-SF.XML.V2021-NOV+ ^[13])	This specification does not depend on a specific version of IC-SF.XML ^[13] ; versions later than version 2021-NOV MAY be used, however, the newest version of IC-SF.XML SHOULD be used as IC-SF.XML is expected to always replace its preceding version. The minimum version was based on technical dependencies on IC-SF.XML; IC-SF.XML is the basic structure of and philosophy behind intelligence community technical specifications.

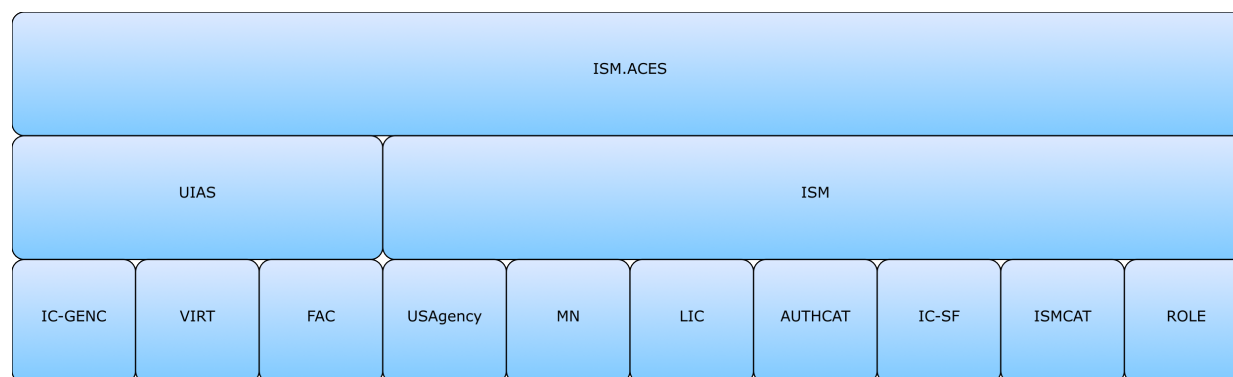


Figure 1 : Related Specifications

1.5.2 - Inverse Dependencies

Generally, it is only necessary to think of the *dependencies* in the dependency tree. However, with the specification versions being decoupled, it is also important to consider the *inverse dependencies*, for compatibility with newer versions of a given specification. The changes introduced to a given specification can sometimes make it incompatible with current versions of its inverse dependencies (specifications that uses the given specification).

This specification is not used by other specifications released by the IC CIO, and therefore does not contain an Inverse Dependency Diagram.

Chapter 2 - Development Guidance

2.1 - Understanding Access Control

This specification participates in the Access Policy leg of the access control framework either as a primary specification or as a dependency of a primary specification. For more information, please see the "Components of Access Control Decisions" chapter in the IC-SF.XML^[13] framework document.

2.2 - Additional Guidance

This section provides additional guidance for encoding data in specific situations. In particular, situations for which there is no clear or single method of encoding the data are documented here. The content of this section will evolve over time as additional situations are identified. Implementers are encouraged to contact the maintainers of this specification for further guidance if necessary.

2.2.1 - The URI

This specification is represented by the Uniform Resource Identifier (URI): urn:us:gov:ic:aces:ism.

This URI is used to reference and denote the application of this ACES.

2.2.2 - Basic Usage

The presence of ISM.XML^[27] data attributes within a data asset specifies that the data asset is controlled by the rules in this ACES and any contextually relevant annexes of this document. This ACES has no need to express information beyond what is already expressed in the ISM.XML^[27] attributes. As such, no specific Need-To-Know Profile is necessary, however, certain ISM.XML^[27] attribute values may have their own requirements for Need-To-Know Profiles.

2.2.3 - Required Conditions for Access

Every condition **MUST** be met prior to access being granted. For example, access to a TS//SI//TK//REL TO USA, CAN/RELIDO resource would require passing the **"TS"**, **"SI"**, **"TK"**, and **"REL"** conditions.

2.2.4 - Non-USA Country Affiliation Access

Access to ISM.XML^[27] documents by an entity whose country affiliation does not contain USA or whose organizational affiliation is not in *CVE Encoding Specification for US Agency Acronyms* (USAgency.CES^[38]), requires the data **MUST** have an foreign disclosure and release marking of either REL TO, EYES or DISPLAY ONLY such that:

- If **"REL"**, the entity **MUST** satisfy the requirements of [Table 30](#).
- If **"EYES"**, the entity **MUST** satisfy the requirements of [Table 32](#).
- If **"DISPLAYONLY"**, the entity **MUST** satisfy the requirements of [Table 36](#).

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the paragraph above, see [Section C.2.1.1 - Non-USA Country Affiliation Access](#).

2.2.5 - Handling Prior CVE Versions

Controlled vocabulary values are mapped to user attributes via an ACES, for the purpose of access control; all access control-relevant values in all current Controlled Vocabulary Enumeration Encoding Specification (CES) are explicitly mapped by an ACES in the Intelligence Community Enterprise Standards Baseline (IC ESB). CESs are retired or replaced, so there is only one version of each vocabulary at a given time. Enterprise systems SHOULD produce and share tagged information using current CESs in accordance with the IC ESB and ICS 500-20, *Intelligence Community Enterprise Standards Compliance* ^[23].

The ACES directly support access decisions based on current CES values. However, existing resources are not necessarily remarked when vocabularies are replaced, and production systems may lag behind the IC ESB. Systems may encounter legacy metadata when making access control decisions.

The office of the IC CIO provides upgrade transforms each time a CES is replaced. Legacy metadata SHOULD be upgraded to current CES values before an access control decision is made. Relevant ACES will explicitly handle current values. Note that it may be necessary to apply a series of upgrade transforms.

2.3 - Need-To-Know and Access Control

This section defines the relationship Need-To-Know Metadata (NTK) has to Information Security Markings (ISM) and Policy Encoding Documents for the purposes of automated access control. An ISM/ NTK access control system relies on three core elements:

1. Markings about the resource such as classification:

ISM represents the security markings describing the classification, dissemination, and caveats about the resource in accordance with the IC Markings System Register & Manual^[9].

NTK represents metadata about a resource that impact an access control decision beyond its ISM classification markings. These metadata may supplement classification markings, as with agency dissemination NTK for ORCON data, or provide other legal, administrative, and/or system-specific information for determining access to a given resource. To ensure data stability, NTK metadata should describe, categorize, label, and refine the resource itself instead of defining the mechanisms by which it is accessed.

Access control policies, including the ACES for ISM, may evolve independently of the data and entity attributes used to enforce them.

2. Markings about the Person or Non-Person Entity (NPE) desiring access:

IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS) is an example of an attribute specification about Persons and NPEs.

3. Rules or policy for granting access based on the markings Access Control Encoding Specification for Information Security Marking (ISM-ACES), NTK Policies):

The ACES associated with ISM is the ISM-ACES.

The ACES associated with NTK is the ISM-ACES, sections on NTK policies and access rules.

NTK metadata is expressed with one or more **ntk:AccessProfile** elements. Each **ntk:AccessProfile** MUST have an **ntk:AccessPolicy** element that contains the Uniform Resource Name (URN) of an access profile for that NTK statement. The **ntk:AccessPolicy** URN may be used to trigger Schematron rules, and it provides a pointer to a specific NTK-related section of the ISM-ACES. Each statement may also contain an **ntk:ProfileDes**, which contains a URN defined in this specification. The **ntk:ProfileDes** may conditionally be required depending on the specific access policy value. A profile Data Encoding Specification (DES) defines structural constraints for an access profile, and the URN may be used to trigger additional Schematron rules. Each **ntk:AccessProfile** must be taken into account for access to a resource based on its location within either the **ntk:RequiresAllOf** element or the **ntk:RequiresAnyOf** element.

If a system receives a resource that is protected with any NTK metadata that is not supported by that system, the resource MUST immediately be rejected, and the system MUST follow [Section 2.4 - Potential Unauthorized Disclosure Data Spill Procedures](#) if:

- The unsupported NTK Access Profile is a member of **ntk:RequiresAllOf** or
- The unsupported NTK Access Profile is a member of an **ntk:RequiresAnyOf** and there are only unsupported NTK Access Profiles as members of the **ntk:RequiresAnyOf**.

2.3.1 - Guidance for systems processing data containing NTK metadata

It is important to note that data may have multiple access system requirements expressed (e.g., system A profile, system B profile, etc.). Each access system requirement is considered separately. Logical structures are used to describe situations where more than one access requirement is needed ("AND"), or where any one of multiple access requirements ("OR") is sufficient for access:

- The element **ntk:RequiresAllOf** indicates that all of the access requirements specified must be satisfied according to the specific NTK-related section of the ISM.ACES^[26] in order to have access to the resource.
- The element **ntk:RequiresAnyOf** is used to indicate that any one of the access requirements must be satisfied according to the specific NTK-related section of the ISM.ACES^[26] in order to have access to the resource.

These logical structures are used within the NTK structure with the following restrictions:

- The **ntk:Access** and **ntk:ExternalAccess** elements must contain either a **ntk:RequiresAllOf** or **ntk:RequiresAnyOf** element as the first child element.
- A **ntk:RequiresAllOf** element may optionally have one **ntk:RequiresAnyOf** child element.
- A **ntk:RequiresAnyOf** element may not include any **ntk:RequiresAllOf** or **ntk:RequiresAnyOf** elements as child elements.
- **ntk:RequiresAllOf** and **ntk:RequiresAnyOf** elements require at least one **ntk:AccessProfile** element as a child element. There may be one or more access elements, each with its own access policy.

Systems handling data containing NTK metadata MUST assess and understand the NTK metadata in order to protect data appropriately. Receiving systems MUST be able to interpret and be authorized for all NTK access profiles necessary to make an access control decision. The following cases detail requirements based on the NTK logic structure:

1. When a logic structure exists indicating all of the access profiles are mandatory, the receiving system MUST be able to interpret access profiles listed within this structure and be able to process access decisions in accordance with associated ISM.ACES^[26] rules. If any NTK metadata is not processable by the system, the system MUST follow [Section 2.4 - Potential Unauthorized Disclosure Data Spill Procedures](#).
2. When a logic structure exists indicating at least one access profile is required, then the receiving system MUST be able to interpret access profiles listed within this structure and be able to process access decisions in accordance with associated ISM.ACES^[26] rules. If no processable NTK metadata exists, the system MUST follow [Section 2.4 - Potential Unauthorized Disclosure Data Spill Procedures](#).

2.4 - Potential Unauthorized Disclosure Data Spill Procedures

If a resource has any unknown metadata required to be understood based on its logic structure, then there is the potential of a data spill. The following steps outline the required actions a system MUST take:

1. The files MUST be segregated and protected via the most restrictive manner available.
2. The cognizant Information Systems Security Manager (ISSM) MUST be contacted.
3. The submitter MUST be contacted to facilitate assessment of the potential spill.

Chapter 3 - Constraints

The ISM.ACES specification expresses many constraints that impact access to data. The ISM.ACES is implied by use of ISM.XML^[27]. Access Control, as referenced in National Institute of Standards and Technology (NIST) 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*^[34], NIST 800-53r4:ACCESS ENFORCEMENT (AC-3) and Flow control, as referenced in NIST 800-53r4^[34], NIST 800-53r4:INFORMATION FLOW ENFORCEMENT (AC-4) are similar in many ways. See chapter [Chapter 5 - Access Control \(AC-3\)](#) for abstract details on Access control and chapter [Chapter 6 - Flow Control \(AC-4\)](#) for abstract details on Flow control. Since part of access control decisions and flow control are the context in which they are made, the guidance in this the following chapters is abstract and any associated concrete mappings can be found in the appendices. The listing of relevant appendices can be found at the end of each chapter in [Section 5.10 - Access Control Specification Specific Mappings](#) and [Section 6.4 - Flow Control Specification Specific Mappings](#).

3.1 - Valid ISM Marked Data

The ISM.ACES only works for valid ISM marked data. Granting access based on invalid ISM.XML^[27] data (data that does not pass Schematron validation) would pose a significant risk.

Chapter 4 - Conformance Validation

An access control decision conforms with this specification if it grants or denies access based on the normative mappings herein. The following steps do not dictate how this validation strategy is implemented.

4.1 - Schema Validation

This specification has no normative schema.

4.2 - Business Rule Validation

Validation MUST ensure access and flow control decisions comply with the business rules expressed in this specification.

Note: The business rules for this specification are expressed in English. The English is normative. As such, any languages or tools may be used to perform the validation as long as the results are consistent with results of the English included in this specification and its dependencies.

Chapter 5 - Access Control (AC-3)

The ISM.ACES specification expresses many constraints that impact access to data. The ISM.ACES is implied by use of ISM.XML^[27]. Since part of access control decisions are the context in which they are made, the guidance in this chapter is abstract and any associated concrete mappings can be found in the appendices. The listing of relevant appendices can be found at the end of this chapter in [Section 5.10 - Access Control Specification Specific Mappings](#).

The associated concrete mappings are normative and MUST be used when applicable. In the absence of an appropriate concrete mapping, the following abstract mapping MAY be used to make the access determination. For ISM.XML^[27] marks not listed below, guidance from the owner of the marking is required to make an access determination. This mapping is used for both Access AC-3 and Flow AC-4 control purposes. For Access, the entity being evaluated is the “final” consumer, specifically the “user” who initiated a request. For Flow, the entity would be the network or System in the “chain” between the final consumer and the user. Different architectures MAY require the immediate adjacent node to be the flow control or MAY require every node to be accounted for. This mapping MAY have applicability for Least Privilege (AC-6), but should be closely scrutinized and differences separately documented and assessed for applicability.

5.1 - Classification

This section describes the mapping of data attributes to a user's/person's clearance or an NPE's accreditation that is determined to be sufficient for access in accordance with E.O. 13526^[4]

5.1.1 - Classification

The guidance in this section applies when the asset is not a JOINT classified resource (i.e. `@ism:joint="true"` is not present). For the *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set* (UIAS.XML^[37]) attributes that implement the abstract person and NPE requirements in the table below, see [Section C.2.2 - Classification](#).

Table 3 - Classification

ISM Attributes	Person or NPE attributes sufficient for access
<code>@ism:classification="TS"</code>	<p>The user has a clearance level of Top Secret.</p> <p>OR</p> <p>The NPE has been accredited to handle Top Secret data.</p>

ISM Attributes	Person or NPE attributes sufficient for access
@ism:classification="S"	<p>The user holds a minimum clearance level of Secret; may have Secret or Top Secret.</p> <p>OR</p> <p>The NPE has been accredited at a minimum to handle Secret data. Accreditation for Secret or Top Secret is acceptable.</p>
@ism:classification="C"	<p>The user holds a minimum clearance level of Confidential; may have Confidential, Secret, or Top Secret.</p> <p>OR</p> <p>The NPE has been accredited at a minimum to handle Confidential data. Accreditation for Confidential, Secret, or Top Secret is acceptable.</p>
@ism:classification="R"	<p>The user holds a minimum clearance level of Confidential; may have Confidential, Secret, or Top Secret.</p> <p>OR</p> <p>The NPE has been accredited at a minimum to handle Restricted data. Accreditation for Restricted, Confidential, Secret, or Top Secret is acceptable.</p>
@ism:classification="U"	<p>No user clearance or system accreditations are required based on classification. However, there may be other restrictions for Controlled Unclassified Information (CUI).</p>

5.1.2 - JOINT Classification

NOTE: "[LIST]" in the following table is used to represent the values of the @ism:ownerProducer attribute. For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.2.3 - JOINT Classification](#).

Table 4 - JOINT Classification

ISM Attributes	Person or NPE attributes sufficient for access
@ism:joint="true" @ism:classification="TS" @ism:ownerProducer="[LIST]"	Requires both: <ul style="list-style-type: none"> • The user's country affiliation is in "[LIST]". • The user has a clearance level of Top Secret issued by their Country Affiliation. OR The NPE has been accredited to handle Top Secret data.
@ism:joint="true" @ism:classification="S" @ism:ownerProducer="[LIST]"	Requires both: <ul style="list-style-type: none"> • The user's country affiliation is in "[LIST]". • The user has a clearance level of Secret or Top Secret issued by their Country Affiliation. OR The NPE has been accredited at a minimum to handle Secret data. Accreditation for Secret or Top Secret is acceptable.
@ism:joint="true" @ism:classification="C" @ism:ownerProducer="[LIST]"	Requires both: <ul style="list-style-type: none"> • The user's country affiliation is in "[LIST]". • The user has a clearance level of Secret or Top Secret issued by their Country Affiliation. OR The NPE has been accredited at a minimum to handle Confidential data. Accreditation for Confidential, Secret, or Top Secret is acceptable.
@ism:joint="true" @ism:classification="U" @ism:ownerProducer="[LIST]"	No user clearance or system accreditations are required based on classification. However, there may be other restrictions for CUI.

5.1.3 - NATO Classification

In this section there is a distinction between general classification levels ("**U**", "**R**", "**C**", "**S**", and "**TS**") and the NATO version of these classifications. For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.2.4 - NATO Classification](#).

NATO values in *CVE Encoding Specification for Fine Access Control* (FAC.CES^[7]) define NATO read-ons for different levels of NATO classification, as follows:

- "**NATO-R**" gives an entity access to NATO data at the Restricted level. A "**NATO-R**" read-on gives access to data that NATO considers to be classified 'NATO RESTRICTED'.
- "**NATO-C**" gives an entity access to NATO data at the Confidential level. A "**NATO-C**" read-on gives access to data that NATO considers to be classified 'NATO CONFIDENTIAL'.
- "**NATO-S**" gives an entity access to NATO data at the Secret level. A "**NATO-S**" read-on gives access to data that NATO considers to be classified 'NATO SECRET'.
- "**NATO-TS**" gives an entity access to NATO data at the Top Secret level. A "**NATO-TS**" read-on gives access to data that NATO considers to be classified 'COSMIC TOP SECRET'.
- There is **no** NATO read-on required for information classified as 'NATO UNCLASSIFIED'.

To understand NATO classification access rules, it is necessary to distinguish the following two cases:

- Case where `@ism:ownerProducer` contains "**NATO**" but does not equal "**NATO**". An example is: `@ism:ownerProducer="USA NATO"`. In this example, the document contains both United States (US) and NATO intelligence. If `@ism:classification="TS"`, assume the US intelligence is "**TS**" but the NATO intelligence is only "**S**". In order to access this document, a PE must have a US "**TS**" clearance but only needs a "**NATO-S**" read-on. The `@ism:highWaterNATO` attribute was created for this case. This document will have `@ism:highWaterNATO="NATO-S"`.
- Case where `@ism:ownerProducer="NATO"`. In this case, there is no ambiguity about the classification of the NATO intelligence, because "**NATO**" is the only value in `@ism:ownerProducer`. For this case, the value of `@ism:classification` determines what level of NATO read-on is required for access.

Table 5 - NATO Classification

ISM Attributes	Person or NPE attributes sufficient for access
@ism:ownerProducer="NATO", @ism:classification="TS"	<p>The user has a read on for access to "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to NATO information at the Top Secret level.</p>
@ism:ownerProducer contains but does not equal "NATO" , @ism:highWaterNATO="TS"	<p>The user has a read on for access to "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to NATO information at the Top Secret level.</p>
@ism:ownerProducer="NATO", @ism:classification="S"	<p>The user has a read on for access to "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to NATO information, at a minimum to handle Secret data. A NATO read on for Secret or Top Secret is acceptable.</p>
@ism:ownerProducer contains but does not equal "NATO" , @ism:highWaterNATO="S"	<p>The user has a read on for access to "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to NATO information, at a minimum to handle Secret data. A NATO read on for Secret or Top Secret is acceptable.</p>
@ism:ownerProducer="NATO", @ism:classification="C"	<p>The user has a read on for access to "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information and accreditation at a minimum to handle Confidential data. A NATO read on for Confidential, Secret or Top Secret is acceptable.</p>

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:ownerProducer contains but does not equal "NATO", @ism:highWaterNATO="C"</p>	<p>The user has a read on for access to "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information and accreditation at a minimum to handle Confidential data. A NATO read on for Confidential, Secret or Top Secret is acceptable.</p>
<p>@ism:ownerProducer="NATO", @ism:classification="R"</p>	<p>The user has a read on for access to "NATO-R", "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information. A NATO read on for Restricted, Confidential, Secret or Top Secret is acceptable.</p>
<p>@ism:ownerProducer contains but does not equal "NATO", @ism:highWaterNATO="R"</p>	<p>The user has a read on for access to "NATO-R", "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information. A NATO read on for Restricted, Confidential, Secret or Top Secret is acceptable.</p>

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:ownerProducer="NATO", @ism:classification="U"</p>	<p>The user MUST be one of:</p> <ul style="list-style-type: none"> Organizational affiliation of US federal government. Organizational affiliation of "USA.SLT" government as defined in E.O. 13549, <i>Executive Order 13549 – Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities</i> [5]. <p>OR</p> <p>The NPE MUST meet minimum security standards required for the handling of NATO information.</p> <div data-bbox="820 850 909 945"></div> <p>Note</p> <p>USA country affiliation is not required.</p>
<p>@ism:ownerProducer contains but does not equal "NATO", @ism:highWaterNATO="U"</p>	<p>The user MUST be one of:</p> <ul style="list-style-type: none"> Organizational affiliation of US federal government. Organizational affiliation of "USA.SLT" government as defined in E.O. 13549, <i>Executive Order 13549 – Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities</i> [5]. <p>OR</p> <p>The NPE MUST meet minimum security standards required for the handling of NATO information.</p> <div data-bbox="820 1575 909 1669"></div> <p>Note</p> <p>USA country affiliation is not required.</p>

5.1.4 - NATO NAC Classification

In this section there is a distinction between NATO classification levels ("U", "R", "C", "S", and "TS") and the NATO North Atlantic Council (NAC) approved cooperative activities version of

these classifications. For the purposes of this section the expression "[NC]" refers to the NAC as encoded for use in ISM.XML^[27]. For example NATO/Partnership for Peace would be "NATO:Partnership_for_Peace". For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.2.5 - NATO NAC Classification](#).



Note



A NATO NAC MAY extend the country affiliation allowed for access beyond NATO. However that expansion would be on a NAC by NAC basis and would require verifying the additional countries with the NAC owners.

Access control rules for NATO NACs use the same two cases as [Section 5.1.3 - NATO Classification](#).

Table 6 - NATO NAC Classification

ISM Attributes	Person or NPE attributes sufficient for access
@ism:ownerProducer="NATO:[NC]", @ism:classification="TS"	The user has a read on for access to "NATO-TS" information. OR The NPE has an accreditation for access to NATO information at the Top Secret level.
@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="TS"	The user has a read on for access to "NATO-TS" information. OR The NPE has an accreditation for access to NATO information at the Top Secret level.
@ism:ownerProducer="NATO:[NC]", @ism:classification="S"	The user has a read on for access to "NATO-S" or "NATO-TS" information. OR The NPE has an accreditation for access to NATO information, at a minimum to handle Secret data. A NATO read on for Secret or Top Secret is acceptable.

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="S"</p>	<p>The user has a read on for access to "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to NATO information, at a minimum to handle Secret data. A NATO read on for Secret or Top Secret is acceptable.</p>
<p>@ism:ownerProducer="NATO:[NC]", @ism:classification="C"</p>	<p>The user has a read on for access to "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information and accreditation at a minimum to handle Confidential data. A NATO read on for Confidential, Secret or Top Secret is acceptable.</p>
<p>@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="C"</p>	<p>The user has a read on for access to "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information and accreditation at a minimum to handle Confidential data. A NATO read on for Confidential, Secret or Top Secret is acceptable.</p>
<p>@ism:ownerProducer="NATO:[NC]", @ism:classification="R"</p>	<p>The user has a read on for access to "NATO-R", "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information. A NATO read on for Restricted, Confidential, Secret or Top Secret is acceptable.</p>

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="R"</p>	<p>The user has a read on for access to "NATO-R", "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information. A NATO read on for Restricted, Confidential, Secret or Top Secret is acceptable.</p>
<p>@ism:ownerProducer "NATO:[NC]", @ism:classification="U"</p>	<p>The user MUST be one of:</p> <ul style="list-style-type: none"> Organizational affiliation of US federal government. Organizational affiliation of "USA.SLT" government. <p>OR</p> <p>The NPE MUST meet minimum security standards required for the handling of NATO information.</p> <div data-bbox="820 1066 906 1159">  </div> <p>Note</p> <p>USA country affiliation is not required.</p>
<p>@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="U"</p>	<p>The user MUST be one of:</p> <ul style="list-style-type: none"> Organizational affiliation of US federal government. Organizational affiliation of "USA.SLT" government. <p>OR</p> <p>The NPE MUST meet minimum security standards required for the handling of NATO information.</p> <div data-bbox="820 1654 906 1747">  </div> <p>Note</p> <p>USA country affiliation is not required.</p>

5.2 - SCI Controls

This section describes the mapping of Sensitive Compartmented Information (SCI) control related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access consistent with the IC Markings System Register specific to Access Rights and Handling (ARH) in the IC Markings, *IC Markings System Register and Manual* [9].



Warning

These instructions only apply to documents using `@ism:SCIcontrols` where the values are contained in the ISM.XML[27] Controlled Vocabulary Enumeration (CVE) *CVEnumISMSCIControls*. Values not in that CVE MAY Require additional user and system accreditation – contact the program manager for guidance.



Note

For Values not in ISM.XML[27] CVE “CVEnumISMSCIControls”, work with standards team if this is required.

For the UIAS.XML[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.3 - SCI Controls](#).

Table 7 - SCI Control Systems

ISM Attributes	Person or NPE attributes sufficient for access
<code>@ism:SCIcontrols</code> contains one or more tokens	<p>The user has been formally granted access into every SCI specified in <code>@ism:SCIcontrols</code>.</p> <p>OR</p> <p>The NPE has been accredited to handle every SCI specified.</p>

5.3 - Special Access Programs

This section is meant to describe the mapping of Special Access Program (SAP) control related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access. However, since the SAP controls are all unpublished and cannot appear in either the ISM.XML[27] CVEnumISMSAR controlled vocabulary or the FAC.CES[7] CVEnumFineAccessControlType controlled vocabulary, detailed guidance regarding the actual SAP values cannot be provided in this specification. Contact the program manager for guidance on how to adapt ISM.XML[27] and FAC.CES[7] for unpublished SAPs that a system is authorized to process.

Abstract logic is provided below to handle the cases of DOD and potentially other agencies' SAPs that have different read-on levels for different classification levels. These rules are based on the following patterns of SAP values in the ISM.XML[27] CVEnumISMSAR controlled vocabulary and the FAC.CES[7] CVEnumFineAccessControlType controlled vocabulary. As noted above, there

currently are no published SAP values in these vocabularies, but general patterns have been defined for values in both vocabularies. See ISM.XML^[27] and FAC.CES^[7].

- **ISM.XML^[27] SAP Pattern:** SAP values in the ISM.XML^[27] controlled vocabulary for SAP markings in `@SARIdentifier` (CVEnumISMSAR) identify, in the following order:

1. The agency that owns the SAP
2. (Optional) The required classification read-on level for the SAP data, for SAPs that have different read-ons for different classification levels
3. The SAP marking value.

Examples of hypothetical SAPs in ISM.XML^[27] are:

- DNI:BUTTER_POPCORN with no classification-level read-on
- DOD:TS:DEMOSAP1, requiring a TS read-on
- DOD:S:DEMOSAP1, requiring a SECRET read-on
- DOD:C:DEMOSAP1, requiring a CONFIDENTIAL read-on.

- **FAC.CES^[7] SAP Pattern:** SAP read-on values in the FAC.CES^[7] controlled vocabulary for Fine Access Controls (CVEnumFineAccessControlType) identify, in the following order:

1. Identification that a Fine Access Controls value is a SAP, signified by initial characters of 'SAR-'
2. The agency that owns the SAP
3. (Optional) The required classification read-on level for the SAP data, for SAPs that have different read-ons for different classification levels
4. The SAP marking value.

Examples of hypothetical SAPs in FAC.CES^[7] are:

- SAR-DNI:BUTTER_POPCORN with no classification-level read-on
- SAR-DOD:TS:DEMOSAP1, signifying the entity has a TS read-on
- SAR-DOD:S:DEMOSAP1, signifying the entity has a SECRET read-on
- SAR-DOD:C:DEMOSAP1, signifying the entity has a CONFIDENTIAL read-on.

For SAPs that have different read-ons for different classification levels, the UIAS.XML^[37] `@fineAccessControls` attribute **MUST** contain denormalized values to facilitate automated access control:

- If a user is granted a TOP SECRET read-on to a hypothetical DOD SAP STORMY PETREL, the user **MUST** have all of the following values in `@fineAccessControls` :
 - "DOD:TS:DEMOSAP1"


- "DOD:S:DEMOSAP1"
- "DOD:C:DEMOSAP1".
- If a user is granted a SECRET read-on to a hypothetical DOD SAP STORMY PETREL, the user **MUST** have all of the following values in **@fineAccessControls** :
 - "DOD:S:DEMOSAP1"
 - "DOD:C:DEMOSAP1".
- If a user is granted a CONFIDENTIAL read-on to a hypothetical DOD SAP STORMY PETREL, the user **MUST** have the following value in **@fineAccessControls** :
 - "DOD:C:DEMOSAP1".

This means that automated access control systems only need to do a simple match of a SAP token to the values in an entity's **@fineAccessControls**. For example, if **@ism:SARIdentifier** contains the token "DOD:S:DEMOSAP1", then a Policy Decision Point (PDP) only needs to check that an entity's **@fineAccessControls** contains "DOD:S:DEMOSAP1". An entity's **@fineAccessControls** will contain "DOD:S:DEMOSAP1" if the entity is briefed into DEMOSAP1 at either the S or TS level.

For a hypothetical Director of National Intelligence (DNI) SAP BUTTER POPCORN that **does not** require different read-ons for different classification levels, an entity **MUST** have a single **@fineAccessControls** value of "DNI:BUTTER_POPCORN".

The abstract logic in the table below defines access rules for SAPs that have different read-ons for different classification levels, and for SAPs that **do not** have different read-ons for different classification levels.

Table 8 - Special Access Programs

ISM Attributes	Person or NPE attributes sufficient for access
@ism:SARIdentifier contains a SAP token that does not include any required classification level.	<p>The user has been read into the unpublished SAP.</p> <p>OR</p> <p>The NPE has been accredited to handle the unpublished SAP data.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:SARIdentifier contains a SAP token that includes a required classification level of TS.</p>	<p>The user has been read into the unpublished SAP at the TS level.</p> <p>OR</p> <p>The NPE has been accredited to handle the unpublished SAP data at the TS level.</p> <div data-bbox="815 541 912 640"></div> <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p>
<p>@ism:SARIdentifier contains a SAP token that includes a required classification level of SECRET.</p>	<p>The user has been read into the unpublished SAP at the S level.</p> <p>OR</p> <p>The NPE has been accredited to handle the unpublished SAP data at the S level.</p> <div data-bbox="815 997 912 1096"></div> <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p>
<p>@ism:SARIdentifier contains a SAP token that includes a required classification level of CONFIDENTIAL.</p>	<p>The user has been read into the unpublished SAP at the C level.</p> <p>OR</p> <p>The NPE has been accredited to handle the unpublished SAP data at the C level.</p> <div data-bbox="815 1449 912 1547"></div> <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p>

5.4 - AEA Controls

This section describes the mapping of Atomic Energy Act (AEA) control related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access consistent with the Atomic Energy Act of 1954.



Note

Foreign disclosure and release determination requires prior approval by DOE (i.e., treat as NOFORN until approval received, if received mark as REL TO).

5.4.1 - Restricted Data (RD)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.1 - Restricted Data \(RD\)](#).

Table 9 - RD

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "RD"	<p>The user has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE RD data.</p>

5.4.2 - Critical Nuclear Weapon Design Information (CNWDI)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.2 - Critical Nuclear Weapons Design Information \(CNWDI\)](#).

Table 10 - RD-CNWDI

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "RD-CNWDI"	<p>The user has been read into CNWDI and has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE RD-CNWDI data.</p>

5.4.3 - RD-SIGMA 14

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.3 - RD-SIGMA 14](#).

Table 11 - RD-SG-14

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "RD-SG-14"	<p>The user has been read into SIGMA 14 and has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE RD-SG 14 data.</p>

5.4.4 - RD-SIGMA 15

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.4 - RD-SIGMA 15](#).

Table 12 - RD-SG-15

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "RD-SG-15"	<p>The user has been read into SIGMA 15 and has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE RD-SG 15 data.</p>

5.4.5 - RD-SIGMA 18

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.5 - RD-SIGMA 18](#).

Table 13 - RD-SG-18

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "RD-SG-18"	<p>The user has been read into SIGMA 18 and has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE RD-SG 18 data.</p>

5.4.6 - RD-SIGMA 20

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.6 - RD-SIGMA 20](#).


Table 14 - RD-SG-20

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "RD-SG-20"	<p>The user has been read into SIGMA 20 and has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE RD-SG 20 data.</p>

5.4.7 - Formerly Restricted Data (FRD)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.7 - Formerly Restricted Data \(FRD\)](#).

Table 15 - FRD

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "FRD"	<p>The presence of FRD does not impact an access control decision. It may impact further handling, use, and releasability decisions.</p> <div>  <p>Warning</p> <p>The presence of a SIGMA with FRD DOES impact Access Control.</p> </div>

5.4.8 - FRD-SIGMA 14

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.8 - FRD-SIGMA 14](#).

Table 16 - FRD-SG-14

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "FRD-SG-14"	<p>The user has been read into SIGMA 14 and has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE FRD-SG 14 data.</p>

5.4.9 - FRD-SIGMA 15

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.9 - FRD-SIGMA 15](#).

Table 17 - FRD-SG-15

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "FRD-SG-15"	<p>The user has been read into SIGMA 15 and has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE FRD-SG 15 data.</p>

5.4.10 - FRD-SIGMA 18

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.10 - FRD-SIGMA 18](#).

Table 18 - FRD-SG-18

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "FRD-SG-18"	<p>The user has been read into SIGMA 18 and has a DOE Q clearance.</p> <p>OR</p> <p>The NPE has been accredited to handle DOE FRD-SG 18 data.</p>

5.4.11 - FRD-SIGMA 20

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.11 - FRD-SIGMA 20](#).


Table 19 - FRD-SG-20

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "FRD-SG-20"	The user has been read into SIGMA 20 and has a DOE Q clearance. OR The NPE has been accredited to handle DOE FRD-SG 20 data.

5.4.12 - DoD Unclassified Controlled Nuclear Information (DCNI)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.12 - DoD Unclassified Controlled Nuclear Information \(DCNI\)](#).


Table 20 - DCNI

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:atomicEnergyMarkings contains "DCNI" and</p> <p>@ism:disseminationControls does not contain "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE has:</p> <ul style="list-style-type: none"> Both duty organizational affiliation and administrative organizational affiliation in "[USAgencyList]" <p>AND</p> <ul style="list-style-type: none"> One of: <ul style="list-style-type: none"> Organizational affiliation of US federal government OR Organizational affiliation of "USA.SLT" government with staff role (i.e., contractors are not authorized). <p>OR</p> <p>The NPE has been accredited to handle DCNI data.</p> <div data-bbox="816 1010 906 1100">  </div> <p>Note</p> <p>USA country affiliation is required because the document is caveated according to the <i>IC Markings System Register and Manual</i> [9] and does not contain any Foreign Disclosure & Release (FD&R) markings, so the document must be handled as NOFORN.</p>
<p>@ism:atomicEnergyMarkings contains "DCNI" and</p> <p>@ism:disseminationControls contains "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE MUST meet:</p> <ul style="list-style-type: none"> If "REL", the entity MUST satisfy the requirements of Table 30. If "EYES", the entity MUST satisfy the requirements of Table 32. If "DISPLAYONLY", the entity MUST satisfy the requirements of Table 36. <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> The NPE MUST be accredited to handle DCNI data.

5.4.13 - DoE Unclassified Controlled Nuclear Information (UCNI)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.13 - DoE Unclassified Controlled Nuclear Information \(UCNI\)](#).

Table 21 - UCNI


ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:atomicEnergyMarkings contains "UCNI" and</p> <p>@ism:disseminationControls does not contain "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE has</p> <ul style="list-style-type: none"> Both duty organizational affiliation and administrative organizational affiliation in "[USAgencyList]" <p>AND</p> <ul style="list-style-type: none"> One of: <ul style="list-style-type: none"> Organizational affiliation of US federal government. Organizational affiliation of "USA.SLT" government with staff role (i.e., contractors are not authorized). <p>OR</p> <p>The NPE has been accredited to handle UCNI data.</p> <div data-bbox="820 1245 909 1339">  </div> <p>Note</p> <p>USA country affiliation is required because the document is caveated according to the <i>IC Markings System Register and Manual</i>^[9] and does not contain any FD&R markings, so the document must be handled as NOFORN.</p>

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:atomicEnergyMarkings contains "UCNI" and</p> <p>@ism:disseminationControls contains "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE MUST meet:</p> <ul style="list-style-type: none"> • If "REL", the entity MUST satisfy the requirements of Table 30. • If "EYES", the entity MUST satisfy the requirements of Table 32. • If "DISPLAYONLY", the entity MUST satisfy the requirements of Table 36. <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> • The NPE MUST be accredited to handle UCNI data.

5.4.14 - Transclassified Foreign Nuclear Information (TFNI)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.5.14 - Transclassified Foreign Nuclear Information \(TFNI\)](#).

Table 22 - TFNI

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:atomicEnergyMarkings contains "TFNI"</p>	<p>The presence of TFNI does not impact an access control decision.</p> <div>  <p>Note</p> <p>It may impact further handling, use, and releasability decisions.</p> </div>



5.5 - Foreign Government Information Markings

This section describes the mapping of Foreign Government related data attributes to a user's/ person's attributes or a NPE's accreditation that are determined to be sufficient for access.

5.5.1 - FGI Protected

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.6.1 - FGI Protected](#).

Table 23 - FGI Protected

ISM Attributes	Person or NPE attributes sufficient for access
@ism:FGISourceProtected equals "FGI"	<p>The presence of FGI protected does not impact an access control decision.</p> <div>  <p>Note</p> <p>It may impact further handling, use, and releasability decisions.</p> </div>
@ism:FGISourceProtected does NOT equal "FGI"	<p>The Access decision logic for FGI is not yet codified in this ACES. The classification and other appropriate markings when revealing the FGI country MUST be determined by the data owner.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

5.5.2 - FGI Open NATO

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.6.2 - FGI Open NATO](#).

Table 24 - FGI Open

ISM Attributes	Person or NPE attributes sufficient for access
@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-TS"	<p>The user has a read on for access to "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to NATO information at the Top Secret level.</p>
@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-S"	<p>The user has a read on for access to "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to NATO information, at a minimum to handle Secret data. A NATO read on for Secret or Top Secret is acceptable.</p>

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-C"</p>	<p>The user has a read on for access to "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information and accreditation at a minimum to handle Confidential data. A NATO read on for Confidential, Secret or Top Secret is acceptable.</p>
<p>@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-R"</p>	<p>The user has a read on for access to "NATO-R", "NATO-C", "NATO-S" or "NATO-TS" information.</p> <p>OR</p> <p>The NPE has an accreditation for access to "NATO" information. A NATO read on for Restricted, Confidential, Secret or Top Secret is acceptable.</p>
<p>@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-U"</p>	<p>The user MUST be one of:</p> <ul style="list-style-type: none"> Organizational affiliation of US federal government. Organizational affiliation of "USA.SLT" government. <p>OR</p> <p>The NPE MUST meet minimum security standards required for the handling of NATO information.</p> <div data-bbox="820 1417 909 1512"> </div> <p>Note</p> <p>USA country affiliation is not required.</p>
<p>@ism:FGISourceOpen does NOT contain "NATO"</p>	<p>The presence of FGI open without NATO does not impact an access control decision.</p> <div data-bbox="820 1669 909 1764"> </div> <p>Note</p> <p>It may impact further handling, use, and releasability decisions.</p>


5.6 - Dissemination Controls

This section describes the mapping of dissemination related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access.

5.6.1 - Risk Sensitive (RS)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.1 - Risk Sensitive \(RS\)](#).

Table 25 - RS

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "RS"	<p>For person entities, the presence of RS does not impact an access control decision.</p> <p>The NPE MUST be accredited to handle RS data.</p> <div>  <p>Note</p> <p>It may impact further handling, use, and releasability decisions. Risk Sensitive has a portion marking of RS but a banner marking of RSEN.</p> </div>

5.6.2 - For Official Use Only (FOUO)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.2 - For Official Use Only \(FOUO\)](#).

Table 26 - FOUO

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:disseminationControls contains "FOUO" and does not contain "REL", "EYES" or "DISPLAYONLY"</p>	<p>The Person Entity (PE) MUST have USA governmental affiliation and be performing duties in service of a USA government organization.</p> <p>OR</p> <p>The NPE MUST meet minimum security standards required for the handling of For Official Use Only (FOUO) data as defined by local USA agency policy.</p> <div data-bbox="820 751 909 846"> </div> <p>Note</p> <p>USA country affiliation is required because the document is caveated according to the <i>IC Markings System Register and Manual</i> [9] and does not contain any FD&R markings, so the document must be handled as NOFORN.</p>
<p>@ism:disseminationControls contains "FOUO" and contains "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE MUST meet:</p> <ul style="list-style-type: none"> • If "REL", the entity MUST satisfy the requirements of Table 30. • If "EYES", the entity MUST satisfy the requirements of Table 32. • If "DISPLAYONLY", the entity MUST satisfy the requirements of Table 36. <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> • The NPE MUST be accredited to handle FOUO data.

5.6.3 - Originator Controlled (OC)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.3 - Originator Controlled \(OC\)](#).

Originator Controlled data (without An Originator Control marking with implied distribution to a pre-determined list of United States Government agencies. (OC-USGOV)) requires the use of Need-To-Know profile "OC-NTK" which details the agencies permitted access by the data's originating agency. There is no direct ISM.XML^[27] to UIAS.XML^[37] mapping. Please see the [Section 5.9.7 -](#)

[Originator Controlled](#) section for guidance on access control decisions related to Originator Controlled (OC) without OC-USGOV.

5.6.4 - Originator Controlled US Government (OC-USGOV)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.4 - Originator Controlled US Government \(OC-USGOV\)](#).

For the purposes of this section, the expression "[USGovList]" refers to the list of organizations in the A designator that refers to a list of United States Government agencies pre-approved for distribution of specially marked Originator Controlled information. (USGOV) Agency Acronym List with namespace urn:us:gov:ic:cvenum:usgovagency:agencyacronym.



Note

The Originator Controlled Need-to-Know (OC-NTK) profile MAY increase the dissemination beyond the default for USGOV. As such, it may be necessary to refer to the Need-To-Know metadata and section [Section 5.9.7 - Originator Controlled](#) for guidance on making an access control decision beyond what is expressed here. This would be true for OC-USGOV that is being distributed to Congressional Intelligence Committees who have oversight functions and responsibilities.

Table 27 - OC-USGOV

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "OC OC-USGOV"	The entity's dutyOrganization exists in "[USGovList]" or in the Need-To-Know metadata block specified on the document as an @ntk:qualifier="originator" or @ntk:qualifier="authorizedDissem" organization.

5.6.5 - Controlled Imagery (IMC)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.5 - Controlled Imagery \(IMC\)](#).

Table 28 - IMC

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "IMC"	<p>For person entities, the presence of IMC does not impact an access control decision. It may impact further handling, use, and releasability decisions.</p> <p>The NPE MUST be accredited to handle IMC data.</p>

5.6.6 - Not Releasable To Foreign Nationals (NF)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.6 - Not Releasable To Foreign Nationals \(NF\)](#).



Warning

Entities eligible for NF data MAY still be ineligible to receive it based on flow control restrictions, see [Chapter 6 - Flow Control \(AC-4\)](#)

Table 29 - NF

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "NF"	<p>For person entities:</p> <p>The user MUST be one of:</p> <ul style="list-style-type: none"> Organizational affiliation of US federal government. Organizational affiliation of "USA.SLT" government. <p>AND</p> <ul style="list-style-type: none"> At least one of the person's countryOfAffiliation MUST be "USA". <p>For NPEs:</p> <p>An NPE MUST satisfy at least one of:</p> <ul style="list-style-type: none"> NPE is accredited for NF (required in cases where non-USA entities have access). ONLY entities with USA country affiliation are authorized for use.

5.6.7 - Caution-Proprietary Information Involved (PR)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.7 - Caution-Proprietary Information Involved \(PR\)](#).

Proprietary Information requires the use of Need-To-Know profile "PROPIN-NTK" which details the users permitted access by the data's owner. Please see the Need-To-Know metadata sections [Section 5.9.9 - Proprietary Information for All US Government Employees](#) and [Section 5.9.10 - Proprietary Information for Specified Members Only](#) for guidance on access control decisions related to Proprietary Information (PROPIN).

5.6.8 - Authorized For Release To (REL)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.8 - Authorized For Release To \(REL\)](#).

For the purposes of this section, the expression "[LIST]" refers to the list of countries within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto. For a breakdown of tetragraph values in "[LIST]", please refer to the Tetragraph Taxonomy in the *CVE Encoding Specification for ISM Country Codes and Tetragraphs* (ISM CAT.CES^[28]) specification.

For the purposes of this section, the expression "**[FullyExpandedList]**" refers to the list of countries that results from expanding the member countries of any tetragraphs in "**[LIST]**" combined with the countries if any in "**[LIST]**". The expansion of the Tetragraphs **MUST** be done by referencing the current ISMCAT.CES^[28]. The concept of decomposability referenced in ISMCAT.CES^[28] is not relevant to access control. All Tetragraphs are able to be expanded to their member countries for the purpose of access control.



Note

For deprecated tetragraph values, if the `@ism:createDate` is earlier than the deprecated date then they are treated the same as a normal tetragraph. If, however, the `@ism:createDate` is after the deprecation has passed then it is invalid ISM. See [Section 3.1 - Valid ISM Marked Data](#) for how this document applies to invalid ISM.



Note

Tetragraph values whose membership is not countries but a descriptive text outlining membership which is not currently machine processable should be ignored for access control decisions.



Warning

Entities eligible for REL data **MAY** still be ineligible to receive it based on flow control restrictions, see [Chapter 6 - Flow Control \(AC-4\)](#)


Table 30 - REL

ISM Attributes	Person or NPE attributes sufficient for access
<code>@ism:disseminationControls</code> contains "REL", <code>@ism:releasableTo</code> =" [LIST] "	<p>The person or NPE MUST meet:</p> <ul style="list-style-type: none"> • At least one Country Affiliation MUST exist in "[FullyExpandedList]". • AND one of: <ul style="list-style-type: none"> • The Administrative Organization affiliation exists in "[USAgencyList]". • The Administrative Organization affiliation is from one of the countries in "[FullyExpandedList]".

5.6.9 - Releasable By Information Disclosure Official (RELIDO)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.9 - Releasable By Information Disclosure Official \(RELIDO\)](#).

Table 31 - RELIDO

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "RELIDO"	<p>The presence of RELIDO does not impact an access control decision.</p> <div data-bbox="815 443 906 533">  </div> <p>Note</p> <p>It may impact further handling, use, and releasability decisions.</p>

5.6.10 - Eyes Only (EYES)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.10 - Eyes Only \(EYES\)](#).

For the purposes of this section, the expression "[LIST]" refers to the list of the Five Eyes Country Trigraphs within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto. The expression "[LIST]" MUST contain "USA" and one or more of the following: "AUS", "CAN", "GBR", or "NZL".



Note

Tetragraph values whose membership is not countries but a descriptive text outlining membership which is not currently machine processable should be ignored for access control decisions.



Warning

Entities eligible for EYES data MAY still be ineligible to receive it based on flow control restrictions, see [Chapter 6 - Flow Control \(AC-4\)](#)

Table 32 - EYES

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "EYES", @ism:releasableTo="[LIST]"	<p>The person or NPE MUST meet:</p> <ul style="list-style-type: none"> • At least one Country Affiliation MUST exist in "[LIST]". • AND one of : <ul style="list-style-type: none"> • The Administrative Organization affiliation exists in "[USAgencyList]". • The Administrative Organization affiliation is from one of the countries in "[LIST]".

5.6.11 - DEA Sensitive (DSEN)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.11 - DEA Sensitive \(DSEN\)](#).

Table 33 - DSEN

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "DSEN" and does not contain "REL", "EYES" or "DISPLAYONLY"	<p>The person MUST meet:</p> <ul style="list-style-type: none"> • If the data is classified, requires clearance level (final) at or above classification marking. • If the data is unclassified, clearance level (final) is not considered. • AND one of: <ul style="list-style-type: none"> • Organizational affiliation of US Federal government. • Organizational affiliation of "USA.SLT" government with staff role (i.e., contractors are not authorized). • AND all of: <ul style="list-style-type: none"> • USA Country Affiliation. • The Administrative Organization exists in "[USAgencyList]". <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> • The NPE, MUST be accredited to handle DSEN data.

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "DSEN" and contains any of "REL", "EYES" or "DISPLAYONLY"	<p>The person or NPE MUST meet:</p> <ul style="list-style-type: none"> If classified, requires clearance level (final) at or above classification marking <p>AND one of:</p> <ul style="list-style-type: none"> Organizational affiliation of US Federal government. Organizational affiliation of "USA.SLT" government with staff role (i.e., contractors are not authorized). <p>• AND any applicable</p> <ul style="list-style-type: none"> If "REL", the user MUST satisfy the requirements of Table 30. If "EYES", the user MUST satisfy the requirements of Table 32. If "DISPLAYONLY", the user MUST satisfy the requirements of Table 36. <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> The NPE MUST be accredited to handle DSEN data.

5.6.12 - Raw Foreign Intelligence Surveillance Act (RAWFISA)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.12 - RAWFISA](#).

Table 34 - RAWFISA

ISM Attributes	Person or NPE attributes sufficient for access
ism:disseminationControls contains "RAWFISA"	<p>For person entities, the presence of RAWFISA does not impact an access control decision. It may impact further handling, use, and releasability decisions.</p> <p>The NPE MUST be accredited to handle RAWFISA data.</p>

5.6.13 - Foreign Intelligence Surveillance Act (FISA)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.13 - Foreign Intelligence Surveillance Act \(FISA\)](#).

Table 35 - FISA

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "FISA" and @ism:classification equal "U"	<p>For person entities, Unclassified data marked for FISA dissemination SHOULD be treated as FOUO. See ISM.ACES entry for Section 5.6.2 - For Official Use Only (FOUO)</p> <p>The NPE MUST be accredited to handle FISA data.</p>
@ism:disseminationControls contains "FISA" and @ism:classification NOT equal "U"	<p>For person entities, the presence of FISA, in classified data, does not impact an access control decision. It may impact further handling, use, and releasability decisions.</p> <p>The NPE MUST be accredited to handle FISA data.</p>

5.6.14 - Authorized For Display But Not Release To (DISPLAYONLY)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.14 - Authorized For Display But Not Release To \(DISPLAYONLY\)](#).

For the purposes of this section the expression "[DLIST]" and "[RLIST]" refers to the list of countries within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto. For a breakdown of tetragraph values in either, please refer to the Tetragraph Taxonomy in the ISMCAT.CES^[28] specification.

For the purposes of this section the expression <tag class="attvalue">[COMPLETE-LIST]</tag> refers to the union of "[DLIST]" and "[RLIST]". If "[RLIST]" does not exist treat "[RLIST]" as an empty set.

For the purposes of this section, the expression "[FullyExpandedList]" refers to the list of countries that results from expanding the member countries of any tetragraphs in <tag class="attvalue">[COMPLETE-LIST]</tag> combined with the countries if any in <tag class="attvalue">[COMPLETE-LIST]</tag>. The expansion of the Tetragraphs MUST be done by referencing the current ISMCAT.CES^[28]. The concept of decomposability referenced in ISMCAT.CES^[28] is not relevant to access control. All Tetragraphs are able to be expanded to their member countries for the purpose of access control.



Note

For deprecated tetragraph values, if the @ism:createDate is earlier than the deprecated date then they are treated the same as a normal tetragraph. If, however, the @ism:createDate is after the deprecation has passed then it is invalid ISM. See [Section 3.1 - Valid ISM Marked Data](#) for how this document applies to invalid ISM.


**Note**

Tetragraph values whose membership is not countries but a descriptive text outlining membership which is not currently machine processable should be ignored for access control decisions.

**Warning**

Entities eligible for DISPLAYONLY data MAY still be ineligible to receive it based on flow control restrictions, see [Chapter 6 - Flow Control \(AC-4\)](#)

Table 36 - DISPLAYONLY

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:disseminationControls contains "DISPLAYONLY", @ism:displayOnlyTo="[DLIST]"</p> <p>Optionally there may be @ism:releasableTo="[RLIST]"</p>	<p>The person meeting the following is granted viewing access, but not the ability to copy, duplicate, or further disseminate the resource in any way.</p> <ul style="list-style-type: none"> • At least one of Country Affiliation MUST exist in "[FullyExpandedList]". • AND One of <ul style="list-style-type: none"> • The Administrative Organization affiliation exists in "[USAgencyList]". • The Administrative Organization affiliation is from one of the countries in "[FullyExpandedList]". <p>The person meeting the following is not impacted by the presence of DISPLAYONLY in any way as they are a US citizen working for the US, Display Only is only a limitation on partners.</p> <ul style="list-style-type: none"> • At least one of countryOfAffiliation MUST be "USA". • AND adminOrganization exists in "[USAgencyList]". <p>The NPE MUST be accredited for DISPLAYONLY or have only persons with USA country affiliation authorized for use.</p> <div data-bbox="816 1392 912 1486">  </div> <p>Warning</p> <p>Access granted by the presence of at least one of the person's or NPE's country affiliation values, or a tetragraph whose membership contains the person's or NPE's country affiliation in the @ism:releasableTo attributes include and exceed that granted by Display Only To and as such the restrictions mentioned here would be superseded by the access granted by Releasable To.</p>

5.6.15 - EXEMPT FROM ICD-501 DISCOVERY

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.7.15 - Exempt from ICD-501 Discovery](#).

Table 37 - EXEMPT FROM ICD501 DISCOVERY

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "EXEMPT_FROM_ICD501_DISCOVERY"	When person or NPE entities submit a search to discover information collected and/or analysis produced in accordance with <i>Discovery and Dissemination or Retrieval of Information within the Intelligence Community</i> ^[17] , the search systems should not return any documents with @ism:disseminationControls contains "EXEMPT_FROM_ICD501_DISCOVERY".

5.7 - Non-IC Dissemination Controls

This section describes the mapping of Non-IC Dissemination control related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access consistent with the IC Markings System Register specific to ARH in the IC Markings^[9].

5.7.1 - Limited Distribution (LIMDIS)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.1 - Limited Distribution \(LIMDIS\)](#).

Table 38 - LIMDIS

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "DS" and @ism:disseminationControls does not contain "REL", "EYES" or "DISPLAYONLY"	<p>The user and NPE MUST meet:</p> <ul style="list-style-type: none"> Organizational affiliation of US Federal government. At least one of the entity's country affiliation MUST be USA. If NPE MUST also be accredited for DS.

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "DS" and @ism:disseminationControls contains "REL", "EYES", or "DISPLAYONLY"	<p>The user and NPE MUST meet:</p> <ul style="list-style-type: none"> Organizational affiliation of US Federal government. If "REL", the entity MUST satisfy the requirements of Table 30. If "EYES", the entity MUST satisfy the requirements of Table 32. If "DISPLAYONLY", the entity MUST satisfy the requirements of Table 36. If NPE MUST be accredited for DS.

5.7.2 - Exclusive Distribution (EXDIS)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.2 - Exclusive Distribution \(EXDIS\)](#).

Table 39 - EXDIS

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "XD"	<p>The user and NPE MUST meet:</p> <ul style="list-style-type: none"> Organizational affiliation of US federal government department or agency as specified by originator. At least one of the entity's country affiliation MUST be USA. If NPE MUST also be accredited for XD.

5.7.3 - No Distribution (NODIS)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.3 - No Distribution \(NODIS\)](#).

Table 40 - NODIS

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "ND"	<p>The user and NPE MUST meet:</p> <ul style="list-style-type: none"> Requires access by named individual. At least one of the entity's country affiliation MUST be USA. If NPE, MUST also be accredited for ND.

5.7.4 - Sensitive But Unclassified (SBU)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.4 - Sensitive But Unclassified \(SBU\)](#).

Table 41 - SBU

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:nonICmarkings contains "SBU" and @ism:disseminationControls does not contain "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE has</p> <ul style="list-style-type: none"> Both duty organizational affiliation and administrative organizational affiliation in "[USAgencyList]" AND The user MUST have Organizational affiliation of US Federal government. <p>OR</p> <p>The NPE MUST meet minimum security standards required for the handling of SBU data.</p> <div data-bbox="820 1024 909 1117"> </div> <p>Note</p> <p>USA country affiliation is required because the document is caveated according to the <i>IC Markings System Register and Manual</i> ^[9] and does not contain any FD&R markings, so the document must be handled as NOFORN.</p>
<p>@ism:nonICmarkings contains "SBU" and @ism:disseminationControls contains "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE MUST meet:</p> <ul style="list-style-type: none"> If "REL", the entity MUST satisfy the requirements of Table 30. If "EYES", the entity MUST satisfy the requirements of Table 32. If "DISPLAYONLY", the entity MUST satisfy the requirements of Table 36. <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> The NPE MUST be accredited to handle SBU data.

5.7.5 - Sensitive But Unclassified NOFORN (SBU-NF)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.5 - Sensitive But Unclassified NOFORN \(SBU-NF\)](#).


Table 42 - SBU-NF

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "SBU-NF"	<p>The user MUST meet:</p> <ul style="list-style-type: none"> Organizational affiliation of US Federal government. At least one of the person's country affiliation MUST be USA. <p>OR</p> <p>An NPE MUST satisfy:</p> <ul style="list-style-type: none"> NPE is accredited for SBU-NF. ONLY NPEs with USA country affiliation are authorized for use.

5.7.6 - Law Enforcement Sensitive (LES)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.6 - Law Enforcement Sensitive \(LES\)](#).

Table 43 - LES

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "LES"	<p>The user MUST be one of:</p> <ul style="list-style-type: none"> Organizational affiliation of US Federal government. Organizational affiliation of "USA.SLT" government. <p>OR</p> <p>The NPE MUST be accredited for LES.</p> <div>  <p>Note</p> <p>USA country affiliation is not required.</p> </div>

5.7.7 - Law Enforcement Sensitive NOFORN (LES-NF)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.7 - Law Enforcement Sensitive NOFORN \(LES-NF\)](#).


Table 44 - LES-NF

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "LES-NF"	<p>The user MUST have at least one country affiliation equal to USA and either have:</p> <ul style="list-style-type: none"> Organizational affiliation of US Federal government. Organizational affiliation of "USA.SLT" government. <p>OR</p> <p>For NPEs:</p> <p>An NPE MUST satisfy:</p> <ul style="list-style-type: none"> NPE is accredited for LES. ONLY entities with USA country affiliation are authorized for use.

5.7.8 - Sensitive Security Information (SSI)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.8 - Sensitive Security Information \(SSI\)](#).

Table 45 - SSI


ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "SSI"	<p>If a person is authorized to access classified national security information, that person is authorized to have access to SSI.</p> <p>The NPE MUST meet minimum security standards required for the handling of SSI data.</p> <div data-bbox="820 577 906 667">  </div> <p>Note</p> <p>USA country affiliation is not required.</p> <p>All products containing SSI need to carry the SSI notice:</p> <p>WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. Parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C.</p>

ISM Attributes	Person or NPE attributes sufficient for access
	552 and 49 C.F.R. Parts 15 and 1520.

5.7.9 - Naval Nuclear Propulsion Information (NNPI)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.9 - Naval Nuclear Propulsion Information \(NNPI\)](#).


Table 46 - NNPI

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonICmarkings contains "NNPI"	<p>The Access decision logic for NNPI is not codified in this ACES.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

5.7.10 - Alternate Compensatory Control Measure (ACCM)

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.8.10 - Alternate Compensatory Control Measure \(ACCM\)](#).

Table 47 - ACCM

ISM Attributes	Person or NPE attributes sufficient for access
Not Supported in ISM.XML ^[27] without extension. Work with standards team if this is required.	<p>The Access decision logic for ACCM is not codified in this ACES.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

5.8 - NATO Controls

This section describes the mapping of NATO control related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access consistent with the IC Markings System Register specific to ARH in the IC Markings^[9].

5.8.1 - ATOMAL

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.9.1 - ATOMAL](#).

Table 48 - ATOMAL

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonUSControls contains "NATO-ATOMAL"	<p>The user has been read into the NATO Control NATO-ATOMAL.</p> <p>OR</p> <p>The NPE has been accredited to handle ATOMAL data.</p>

5.8.2 - BALK

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.9.2 - BALK](#).

Table 49 - BALK

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonUSControls contains "NATO-BALK"	<p>The user has been read into the NATO Control NATO-BALK.</p> <p>OR</p> <p>The NPE has been accredited to handle BALK data.</p>

5.8.3 - BOHEMIA

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section C.9.3 - BOHEMIA](#).

Table 50 - BOHEMIA

ISM Attributes	Person or NPE attributes sufficient for access
@ism:nonUSControls contains "NATO-BOHEMIA"	<p>The user has been read into the NATO Control NATO-BOHEMIA.</p> <p>OR</p> <p>The NPE has been accredited to handle BOHEMIA data.</p>

5.9 - Need-To-Know Access Control

Each sub-section in this section is identified by a URN. When used as the value of an **ntk:AccessPolicy** element in an Need-To-Know XML assertion, the URN specifies that the protected resource is subject to the access controls encoded in the corresponding section of this chapter and contextually relevant annexes of this document. This document provides access control encoding for Need-To-Know XML access profiles listed in [Table 51](#). For information about each Need-to-Know Access Profile, see the Need-To-Know XML.

Table 51 - Need-To-Know Access Policies

Access Policy URN	Associated Access Profile
urn:us:gov:ic:aces:ntk:xd	Exclusive Distribution
urn:us:gov:ic:aces:ntk:ico	Intelligence Community Only
urn:us:gov:ic:aces:ntk:license	Licensing Agreements
urn:us:gov:ic:aces:ntk:mn	Mission Need
urn:us:gov:ic:aces:ntk:nd	No Distribution
urn:us:gov:ic:aces:ntk:oc	Originator Controlled
urn:us:gov:ic:aces:ntk:permissive	Permissive Groups and Individuals
urn:us:gov:ic:aces:ntk:propin:1	Proprietary Information for All Government Employees
urn:us:gov:ic:aces:ntk:propin:2	Proprietary Information for Specified Members Only
urn:us:gov:ic:aces:ntk:rac	Restricted Authority Category
urn:us:gov:ic:aces:ntk:restrictive	Restrictive Groups
urn:us:gov:ic:aces:ntk:role:enterprise:role	Enterprise Role

The access control encodings in this document rely solely on information in (1) an Need-to-Know Access Profile and (2) related controls expressed in ISM.XML^[27] attributes. For the evaluation of an access decision for a particular Need-To-Know XML assertion, a PDP must have the entire related Need-To-Know access profile, all ISM.XML^[27] attributes associated with the resource, and

an entity's attributes. The access determination for any particular Need-To-Know access profile may be part of a larger access control decision.

The guidance in this section is abstract and maps Need-To-Know XML metadata to abstract entity concepts. However, part of an access control decision is the context in which it is made, and any associated concrete mappings can be found in the appendices. The associated concrete mappings are normative and **MUST** be used when applicable. In the absence of an appropriate concrete mapping, the following abstract mapping **MAY** be used to make an access determination.



Note

Some Need-To-Know Access Profiles support requirements of the IC Markings^[9]. Other Need-To-Know Access Profiles support policy in ICPG 710.1, *Application of Dissemination Controls: Originator Control*^[20]. Some Need-To-Know Access Profiles are provided to meet a mission need and are not based on a specific policy.

5.9.1 - Enterprise Role

The Enterprise Role Access Policy is identified by the URN
"urn:us:gov:ic:aces:ntk:role:enterprise:role".

For the ROLE.XML that implement the enterprise role entity requirements in the table below, see .

Table 52 - Enterprise Role Access List

NTK Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the Enterprise Role list URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:role:enterprise:role </ntk:AccessPolicy></pre>	The person or NPE MUST be associated with and performing activities under the ROLE categories specified in the ntk:AccessProfileValues .
ntk:ProfileDes contains the ROLE URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:role </ntk:ProfileDes></pre>	
one to many Enterprise Role lists <pre><ntk:AccessProfileValue ntk:vocabulary="role:enterpriseRole" >[ALEP]</ntk:AccessProfileValue></pre>	

5.9.2 - Exclusive Distribution

The Exclusive Distribution (EXDIS) Access Policy is identified by the URN
"urn:us:gov:ic:aces:ntk:xd".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.2 - Mapping EXDIS to UIAS](#).



Note

- In the following table, the "[ORIG_AGENCY]" and "[DISSEM_AGENCY]" tokens are placeholders for actual agency acronyms.

Table 53 - EXDIS Access List

Need-To-Know Access Profile	Entity Attribute
ntk:AccessPolicy contains the EXDIS URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:xd </ntk:AccessPolicy></pre>	The person or NPE MUST meet <i>at least one</i> of these criteria: <ol style="list-style-type: none"> 1. The person or NPE's duty organization matches "[ORIG_AGENCY]". 2. The person or NPE's duty organization matches one of "[DISSEM_AGENCY]".
ntk:ProfileDes contains the Agency Dissem URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:agencydissem </ntk:ProfileDes></pre>	
exactly one originator agency <pre><ntk:AccessProfileValue ntk:qualifier="originator" ntk:vocabulary="organization:usa-agency" >[ORIG_AGENCY]</ntk:AccessProfileValue></pre>	
zero to many dissemto agencies <pre><ntk:AccessProfileValue ntk:qualifier="dissemto" ntk:vocabulary="organization:usa-agency" >[DISSEM_AGENCY]</ntk:AccessProfileValue></pre>	

5.9.3 - Intelligence Community Only

The Intelligence Community Only (ICO) Access Policy is identified by the URN "urn:us:gov:ic:aces:ntk:ico".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.3 - Mapping ICO to UIAS](#).

Table 54 - Restriction to IC Members

Need-To-Know Access Profile	Abstract Person Attributes
ntk:AccessPolicy contains the ICO URN <pre><ntk:AccessProfile ism:classification="U" ism:ownerProfile="USA"> <ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:ico </ntk:AccessPolicy> </ntk:AccessProfile></pre>	The person or NPE MUST be a member of the Intelligence Community.

5.9.4 - License

The License Access Policy is identified by the URN "urn:us:gov:ic:aces:ntk:license".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.4 - Mapping LICENSE to UIAS](#).

Table 55 - LICENSE-NTK Access List



Need-To-Know Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the License URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:license </ntk:AccessPolicy></pre>	The person or NPE MUST meet all of these criteria: <ol style="list-style-type: none"> 1. If [OSC-CommercialOpenSource1] is one of the "[LICENSE]" values, the person or NPE MUST be a member of the Intelligence Community. 2. The person or NPE MUST meet the requirements for all other license agreements as indicated by the set of "[LICENSE]" values.
ntk:ProfileDes contains the Data Sphere URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:datasphere </ntk:ProfileDes></pre>	
one to many licenses <pre><ntk:AccessProfileValue ntk:vocabulary="datasphere:license" >[LICENSE]</ntk:AccessProfileValue></pre>	

5.9.5 - Mission Need

The Mission Need Access Policy is identified by the URN "urn:us:gov:ic:aces:ntk:mn".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.5 - Mapping MN to UIAS](#).

Table 56 - MN-NTK Access List

Need-To-Know Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the Mission Need Profile (MN) URN	The person or NPE MUST meet <i>both</i> the issue and region criteria:
<pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:mn </ntk:AccessPolicy></pre>	Issue Criteria. If MN issues are listed in the Need-To-Know Access Profile, the user or NPE MUST have an association with at least one of the listed "[ISSUE]" values.
ntk:ProfileDes contains the Data Sphere URN	 Note If no MN issues are listed in NTK, there is no issue restriction.
<pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:datasphere </ntk:ProfileDes></pre>	
zero to many MN issues	Region Criteria. If MN regions are listed in the Need-To-Know Access Profile, the user or NPE MUST have an association with at least one of the listed "[REGION]" values.
<pre><ntk:AccessProfileValue ntk:vocabulary="datasphere:mn:issue" >[ISSUE]</ntk:AccessProfileValue></pre>	
zero to many MN regions	 Note If no MN regions are listed in NTK, there is no region restriction.
<pre><ntk:AccessProfileValue ntk:vocabulary="datasphere:mn:region" >[REGION]</ntk:AccessProfileValue></pre>	

5.9.6 - No Distribution

The Data Encoding Specification for No Distribution Need-To-Know (NODIS) Access Policy is identified by the URN "**urn:us:gov:ic:aces:ntk:nd**".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.6 - Mapping NODIS to UIAS](#).

Table 57 - ND-NTK Access List

Need-To-Know Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the NODIS URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:nd </ntk:AccessPolicy></pre>	The user or NPE MUST meet <i>at least one</i> of these criteria: <ol style="list-style-type: none"> One or more groups are listed in the NTK Access Profile and the person or NPE has an association with at least one [GRP_VALUE] from the appropriate system identified by group:[GRP_VOCAB]. One or more individuals are listed in the NTK Access Profile and the person matches the [IND_VALUE] from the appropriate system identified by individual:[IND_VOCAB].
ntk:ProfileDes contains the Group & Individual URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre>	
zero to many groups <pre><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" > [GRP_VALUE] </ntk:AccessProfileValue></pre>	
zero to many individuals <pre><ntk:AccessProfileValue ntk:vocabulary="individual:[IND_VOCAB]" > [IND_VALUE] </ntk:AccessProfileValue></pre>	

5.9.7 - Originator Controlled

The ORCON Access Policy is identified by the URN "urn:us:gov:ic:aces:ntk:oc".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.7 - Mapping ORCON to UIAS](#).



Note

- The ISM.ACES ORCON access rule does not apply in a Secure Community of Interest (SCOI) and SCOI policies should be used instead. In a SCOI, the ORCON-NTK in a document should not be used for automated access decisions and instead use the list of authorized members of the SCOI.

Table 58 - ORCON Access Control Mapping

Need-To-Know Access Profile	Entity Attribute
ntk:AccessPolicy contains the ORCON URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:oc </ntk:AccessPolicy></pre>	The user or NPE MUST meet <i>at least one</i> of these criteria: <ol style="list-style-type: none"> 1. The person or NPE's duty organization matches "[ORIG_AGENCY]". 2. The person or NPE's duty organization matches one of "[DISSEM_AGENCY]".
ntk:ProfileDes contains the Agency Dissem URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:agencydissem </ntk:ProfileDes></pre>	
exactly one originator agency <pre><ntk:AccessProfileValue ntk:qualifier="originator" ntk:vocabulary="organization:usa-agency" >[ORIG_AGENCY]</ntk:AccessProfileValue></pre>	
zero to many dissemto agencies <pre><ntk:AccessProfileValue ntk:qualifier="dissemto" ntk:vocabulary="organization:usa-agency" >[DISSEM_AGENCY]</ntk:AccessProfileValue></pre>	

5.9.8 - Permissive

The Permissive Access Policy is identified by the URN
"urn:us:gov:ic:aces:ntk:permissive".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.8 - Mapping Permissive to UIAS](#).

Table 59 - Permissive Access Control Mapping

Need-To-Know Access Profile	Entity Attribute
ntk:AccessPolicy contains the Permissive URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:permissive </ntk:AccessPolicy></pre>	The user or NPE MUST meet <i>at least one</i> of these criteria: <ol style="list-style-type: none"> One or more groups are listed in the NTK Access Profile and the person or NPE has an association with at least one [GRP_VALUE] from the appropriate system identified by group:[GRP_VOCAB]. One or more individuals are listed in the NTK Access Profile and the person matches the [IND_VALUE] from the appropriate system identified by individual:[IND_VOCAB].
ntk:ProfileDes contains the Group & Individual URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre>	
zero to many groups <pre><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ntk:AccessProfileValue></pre>	
zero to many individuals <pre><ntk:AccessProfileValue ntk:vocabulary="individual:[IND_VOCAB]" >[IND_VALUE]</ntk:AccessProfileValue></pre>	

5.9.9 - Proprietary Information for All US Government Employees

The All US Government Employees PROPIN Access Policy is identified by the URN "urn:us:gov:ic:aces:ntk:propin:1".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.9 - Mapping PROPIN to UIAS](#).

Table 60 - All US Government Employee PROPIN Access List

NTK Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the All USG PROPIN URN <pre><ntk:AccessProfile ism:classification="U" ism:ownerProducer="USA"> <ntk:AccessPolicy >urn:us:gov:ic:aces:ntk:propin:1 </ntk:AccessPolicy> </ntk:AccessProfile></pre>	The person or NPE MUST be a US Government employee or member of the US military.

NTK Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the All USG PROPIN URN	The Person or NPE MUST meet <i>at least one</i> of the following criteria:
<pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:propin:1 </ntk:AccessPolicy></pre>	1. The person or NPE is a US Government employee or member of the US military.
ntk:ProfileDes containing the Group & Individual URN	2. One or more groups are listed in the NTK Access Profile and the person or NPE has an association with at least one [GRP_VALUE] from the appropriate system identified by group:[GRP_VOCAB].
<pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre>	
zero or more groups	
<pre><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ntk:AccessProfileValue></pre>	3. One or more individuals are listed in the NTK Access Profile and the person matches the [IND_VALUE] from the appropriate system identified by individual:[IND_VOCAB].
zero or more individuals	
<pre><ntk:AccessProfileValue ntk:vocabulary="individual:[IND_VOCAB]" >[IND_VALUE]</ntk:AccessProfileValue></pre>	

5.9.10 - Proprietary Information for Specified Members Only

The Specified Members Only PROPIN Access Policy is identified by the URN

"urn:us:gov:ic:aces:ntk:propin:2"

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.9 - Mapping PROPIN to UIAS](#).

Table 61 - Group PROPIN Access List

NTK Access Profile	Person or NPE Attributes
<p>ntk:AccessPolicy contains the Specified Members Only PROPIN URN</p> <pre data-bbox="196 415 928 510"><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:propin:2 </ntk:AccessPolicy></pre> <p>ntk:ProfileDes containing the Group & Individual URN</p> <pre data-bbox="196 638 928 732"><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre> <p>zero or more groups</p> <pre data-bbox="196 827 928 921"><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ntk:AccessProfileValue></pre> <p>zero or more individuals</p> <pre data-bbox="196 1016 928 1110"><ntk:AccessProfileValue ntk:vocabulary="individual:[IND_VOCAB]" >[IND_VALUE]</ntk:AccessProfileValue></pre>	<p>The Person or NPE MUST meet <i>at least one</i> of the following criteria:</p> <ol style="list-style-type: none"> 1. One or more groups are listed in the NTK Access Profile and the person or NPE has an association with at least one [GRP_VALUE] from the appropriate system identified by group:[GRP_VOCAB]. 2. One or more individuals are listed in the NTK Access Profile and the person matches the [IND_VALUE] from the appropriate system identified by individual:[IND_VOCAB].

5.9.11 - Custom Profiles for PROPIN

When existing PROPIN profiles are insufficient for protecting PROPIN information, it is expected that a custom profile will be created. There are some restrictions to custom profiles that MUST be adhered to in order to comply with enterprise standards:

- The **ntk:AccessPolicy** URN MUST start with:
"urn:us:gov:ic:aces:ntk:propin:".
- The characters following the predefined beginning of the PROPIN-NTK URI are used to uniquely identify the custom profile and MUST NOT be purely numeric unless previously coordinated with the IC CIO Technical Specifications team. Numeric entries are restricted to enterprise PROPIN-NTK profiles to prevent collisions with custom profiles. Combinations of numbers and letters are allowed as long as the extension starts with at least one alphabetic character.

5.9.12 - Restricted Authority Category

The Restricted Authority Category (RAC) Access Policy is identified by the URN
"urn:us:gov:ic:aces:ntk:rac".

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.10 - Mapping RAC to UIAS](#).

Table 62 - RAC-NTK Access List

NTK Access Profile	Person or NPE Attributes
ntk:AccessPolicy contains the RAC list URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:rac </ntk:AccessPolicy></pre>	The person or NPE MUST be associated with and performing activities under the authority categories specified in the ntk:AccessProfileValues .
ntk:ProfileDes contains the Data Sphere URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:datasphere </ntk:ProfileDes></pre>	
one to many RAC lists <pre><ntk:AccessProfileValue ntk:vocabulary="datasphere:rac" >[RAC]</ntk:AccessProfileValue></pre>	

5.9.13 - Restrictive

The Restrictive Access Policy is identified by the URN
"urn:us:gov:ic:aces:ntk:restrictive"

For the UIAS.XML^[37] attributes that implement the abstract entity requirements in the table below, see [Section C.10.11 - Mapping Restrictive to UIAS](#).

Table 63 - Restrictive Access Control Mapping

NTK Access Profile	Entity Attribute
ntk:AccessPolicy contains the Restrictive URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:restrictive </ntk:AccessPolicy></pre>	The Person or NPE MUST have an association with <i>all</i> groups specified in ntk:AccessProfileValues such that they are a member of the group [GRP_VALUE] from the system identified by group:[GRP_VOCAB].
ntk:ProfileDes contains the Group & Individual URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre>	
zero to many groups	
<pre><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ntk:AccessProfileValue></pre>	

5.10 - Access Control Specification Specific Mappings

For mappings to specific specifications for the concepts covered in this chapter, please refer to the following appendices:

- Mapping ISM.XML^[27] and UIAS.XML^[37] [Appendix C - Mapping ISM and UIAS Access & Flow](#)

Chapter 6 - Flow Control (AC-4)

6.1 - Introduction

Flow control AC-4 is required in instances when an entity, based on its UIAS.XML^[37] attributes, is granted access to an object under AC-3, but its current environment or other localized context SHOULD prohibit the entity from receiving the object.

This section is currently only applicable to systems that know they are dealing with users who have non ICPKI certificates. A system that is receiving federated requests and believes those requests are always coming from a known network MAY ignore these restrictions. A system that has a user directly connecting SHOULD have both of these values available and SHOULD be making decisions based on them for that interaction.



Warning

Ignoring these restrictions is a risk posture decision for each system to make. Without these restrictions if the system receives federated queries they may be putting themselves at risk of spilling NF or partner restricted data.

Examples of AC-4 Flow control:

1. A user with a TS clearance being granted access to TS data from a workstation that can only process SECRET information. The TS data can't be sent to the user even though the user has passed the access control requirements.
2. A user with a **countryOfAffiliation** of "USA" requests "NOFORN" information on a network that is "REL ACGU". Even though the user should have access to the data under AC-3, the user is on a network that cannot protect the data securely.
3. Assume an interaction among:
 - System A with trust chain including Authority 1 and Authority 2.
 - System B with trust chain including only Authority 1.
 - User with a certificate signed by Authority 2.

If the user directly connects to System A, the connection is successful. Then System A using its Authority 1 certificate makes a request of System B only passing the DN of the user to System B. System B will accept the connection from System A but will not be able to determine the certificate authority of the user whose DN was passed based on the connection with System A, unless System A passes that information in the request to System B.

There are currently two (2) concepts that are being codified as Flow control unique concepts, that is they do not participate in the AC-3 decision but are necessary for AC-4.

- Certificate Authority
- Originating Network

In contrast to the Access control chapter this chapter will have the more concrete Person or NPE attributes sufficient for access on the left and the more abstract Information Resource (as defined by ICS 500-20^[23]). Attributes on the right, as shown in tables [Table 65](#) and [Table 66](#).

A summary of the flow controls can be found in [Table 64](#). Table cells with “N/A” indicate they are not an anticipated intersection of Certificate Authority and Network.


Table 64 - Flow Control Summary

Network	Unknown	ICPKI	CADPKI
Unknown	At a minimum all data is releasable to all of USA, AUS, CAN, GBR, NZL	At a minimum all data is releasable to all of USA, AUS, CAN, GBR, NZL	At a minimum all data is releasable to all of USA, AUS, CAN, GBR, NZL
IMIS	At a minimum all data is releasable to all of USA, AUS, GBR	N/A	At a minimum all data is releasable to all of USA, AUS, GBR
QNET	At a minimum all data is releasable to all of USA, AUS, GBR	N/A	At a minimum all data is releasable to all of USA, AUS, GBR
NSANet	At a minimum all data is releasable to all of USA, AUS, CAN, GBR, NZL	The data MAY be NOFORN	At a minimum all data is releasable to all of USA, AUS, CAN, GBR, NZL
JWICS	At a minimum all data is releasable to all of USA, AUS, CAN, GBR, NZL	The data MAY be NOFORN	At a minimum all data is releasable to all of USA, AUS, CAN, GBR, NZL

6.2 - Certificate Authority

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section D.2 - Certificate Authority](#).


Table 65 - Certificate Authority

Person or NPE attributes sufficient for access	Information Resource Attributes
The certificate Authority is Unknown	<p>The resource MUST not be NF.</p> <div>  <p>Warning</p> <p>As Certificate Authority is optional a system MAY not have access to it. Lacking such information a system MUST not grant access to NF data.</p> </div>
The certificate Authority is ICPKI	The resource is not constrained by the PKI authority.
The certificate Authority is CADPKI	The resource MUST not be NF.

6.3 - Originating Network

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section D.3 - Originating Network](#).

Table 66 - Originating Network

Person or NPE attributes sufficient for access	Information Resource Attributes
The Originating Network is Unknown	<p>The resource MUST be approved for Release to at least USA, AUS, CAN, GBR, and NZL.</p> <div>  <p>Warning</p> <p>As Originating Network is optional a system MAY not have access to it. Lacking such information a system MUST not grant access to data marked USA, AUS, CAN, GBR, NZL.</p> </div>
The Originating Network is IMIS	The resource MUST be approved for Release to at least USA, AUS, GBR.
The Originating Network is QNET	The resource MUST be approved for Release to at least USA, AUS, CAN, GBR, NZL.
The Originating Network is NSANET	The resource does not have any network based flow control.
The Originating Network is JWICS	The resource does not have any network based flow control.

6.4 - Flow Control Specification Specific Mappings

For mappings to specific specifications for the concepts covered in this chapter, please refer to the following appendices:

- Mapping ISM.XML^[27] and UIAS.XML^[37] [Appendix D - Mapping ISM and UIAS Flow Control](#).

Appendix A Feature Summary

The following tables summarize major features by version for ISM.ACES. The “Required date” is the date when systems SHOULD support a feature based on the specified driver. Executive Orders, Information Security Oversight Office (ISOO) notices, ICDs and other policy documents have a variety of effective dates. The “Required date” may be later than the date of applicable policy based on the effective date defined in the policy (e.g., The IC Markings^[9] has an implementation date of one year after issuance).

Table 67 - Feature Summary Legend

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can’t comply)
N/A	Not Applicable. Feature is no longer required.
Cell Colors represent the same information as the Key value	

A.1. ISM.ACES Feature Comparison

A.1.1. Features from V2019-MARr2019-JUN to V2021-NOV

Table 68 - ISM.ACES Feature Comparison V2019-MARr2019-JUN to V2021-NOV

Required date	Feature	V2019-MARr2019-JUN	V2019-SEP	V2020-OCT	V2021-NOV
	Support hierarchical SCIs	N	F	F	F
	Remove special access logic rules for HCS. HCS now operates like other SCIs.	N	F	F	F
	Support for the August 2019 version of the IC Markings Register and Manual	N	N	F	F
	Update NATO access rules to represent four levels of NATO read-on and a new @ism:highWaterNATO attribute.	N	N	N	F
	Incorporate DOD Special Access Program Control Office (SAPCO) guidance on SAPs	N	N	N	F
	Add access rules for new Exempt From ICD 501 Discovery dissemination control	N	N	N	F

A.1.2. Features from 2018-AUG to V2019-MARr2019-JUN

Table 69 - ISM.ACES Feature Comparison 2018-AUG to V2019-MARr2019-JUN

Required date	Feature	2018-AUG	2018-NOV	V2019-MAR	V2019-MARr2019-JUN
IC Marking System Register and Manual 30 August 2019 ^[9]	Support RAW-FISA dissemination control	N	F	N	F
	NTK Access Controls consolidated into ISM.XML ^[27]	N	N	F	F

A.1.3. Features from 2016-DEC to 2018-AUG

Table 70 - ISM.ACES Feature Comparison 2016-DEC to 2018-AUG

Required date	Feature	2016-DEC	2017-JUL	2018-APR	2018-AUG
	Move ECRU and NONBOOK under SI and remove ENDSEAL	N	F	F	F

A.1.4. Features from 2014-DEC to 2016-DEC

Table 71 - ISM.ACES Feature Comparison 2014-DEC to 2016-DEC

Required date	Feature	2014-DEC	2015-AUG	2016-SEP	2016-DEC
IC Marking System Register and Manual 24 December 2015 ^[9]	Restrict EYES to one or more of Five Eyes Country Trigraphs	N	F	F	F
	Restrict FISA to at least same access control as FOUO	N	F	F	F
	Decomposability of Tetragraphs	N	N	F	F
	Describe handling control requirements for NPEs	P	P	F	F
IC Marking System Register and Manual 30 June 2016 ^[9]	Move KDK subs under TK	N	N	F	F
	Account for 2nd Party Integrees in releasability access logic	N	N	P	F

A.1.5. Features from V1 to 2014-DEC

Table 72 - ISM.ACES Feature Comparison V1 to 2014-DEC

Required date	Feature	V1	V2	2014-DEC
	Codify RS, FISA, IMC, and TFNI	N	F	F
	Fine Access Control	N	F	F
	Flow Control for originatingNetwork and issuingCertificate Authority	N	N	F
	Handle NATO as a read-on	N	N	F
	Codify FGI Protected, FGI Open NATO, LIMDIS, EXDIS, NODIS, LES, LES-NF, NNPI, ACCM	N	N	F

A.1.5.1. Features Partial and N/A from V1 to 2014-DEC

Table 73 - ISM.ACES Feature Comparison V1 to 2014-DEC

Required date	Feature	V1	V2	2014-DEC
	Describe handling control requirements for NPEs	P	P	P

Appendix B Change History

The following table summarizes the version identifier history for this DES.

Table 74 - DES Version Identifier History

Version	Date	Purpose
1	September 6, 2013	Initial Release
2	March 14, 2014	Routine revision to technical specification. For details of changes, see Section B.14 - V2 Change Summary
2014-DEC	December 4, 2014	Routine revision to technical specification. For details of changes, see Section B.13 - V2014-DEC Change Summary
2015-AUG	August 13, 2015	Routine revision to technical specification. For details of changes, see Section B.12 - V2015-AUG Change Summary
2016-SEP	September 9, 2016	Routine revision to technical specification. For details of changes, see Section B.11 - V2016-SEP Change Summary
2016-DEC	December 19, 2016	Routine revision to technical specification. For details of changes, see Section B.10 - V2016-DEC Change Summary
2017-JUL	July 21, 2017	Routine revision to technical specification. For details of changes, see Section B.9 - V2017-JUL Change Summary
2018-APR	April 20, 2018	Routine revision to technical specification. For details of changes, see Section B.8 - V2018-APR Change Summary
2018-AUG	August 31, 2018	Routine revision to technical specification. For details of changes, see Section B.7 - V2018-AUG Change Summary
2018-NOV	November 26, 2018	Routine revision to technical specification. For details of changes, see Section B.6 - V2018-NOV Change Summary
2019-MAR	March 8, 2019	Routine revision to technical specification. For details of changes, see Section B.5 - V2019-MAR Change Summary
2019-MARr2019-JUN	June 13, 2019	Routine revision to technical specification. For details of changes, see Section B.4 - V2019-MARr2019-JUN Change Summary
2019-SEP	September 6, 2019	Routine revision to technical specification. For details of changes, see Section B.3 - V2019-SEP Change Summary

Version	Date	Purpose
2020-OCT	October 1, 2020	Routine revision to technical specification. For details of changes, see Section B.2 - V2020-OCT Change Summary
2021-NOV	December 3, 2021	Routine revision to technical specification. For details of changes, see Section B.1 - V2021-NOV Change Summary

B.1 - V2021-NOV Change Summary

Significant drivers for version 2021-NOV include:

- Community change requests.

[Table 75](#) summarizes the changes made to this technical specification from version 2019-SEP to version 2021-NOV.

Table 75 - V2021-NOV Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Add Enterprise Role access profile into ISM for ALEP attribute (CR-2019-013).	Documentation	No impact to systems.
2	Resolve inconsistency in ISM-ACES Rules for FOUO (CR-2018-122).	Documentation	No impact to systems.
3	Modify ISM-ACES Rules to Account for dutyOrganization and adminOrganization values for Foreign Partners (CR-2021-004).	Documentation	No impact to systems.
4	Update FAC value of NATO to represent four levels of NATO read-on: NATO-R, NATO-C, NATO-S and NATO-TS (CR-2020-005). New <code>@ism:highWaterNATO</code> attribute.	Documentation	No impact to systems.
5	Modify handling of SAP accesses to support DOD SAPCO rules. (CR-2021-024)	Documentation	Identity, Credential, and Access Management (ICAM) systems need to be updated to accommodate this change
6	Add access control rules for new Exempt From ICD 501 Discovery dissemination control (CR-2021-026)	Documentation	ICAM systems need to be updated to accommodate this change.

#	Change	Artifacts Changed	Compatibility Notes
7	Remove the ACSS PKI CA from the ISM-ACES DES (CR-2021-021)	Documentation	No impact to systems.

B.2 - V2020-OCT Change Summary

Significant drivers for version 2020-OCT include:

- August 2019 version of the IC Markings Register and Manual.

[Table 76](#) summarizes the changes made to this technical specification from Version 2019-SEP to Version 2020-OCT.

Table 76 - V2020-OCT Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Modified for August 2019 Register and Manual. Changes to SCI Controls: BUR, HCS, KLM, MARVEL, and RSV. Change to PROPIN access policy. Removed one dissemination control. (CR-2019-163, CR-2020-018)	Documentation	No impact to systems.
2	Change sub-compartment to subcompartment for ISM and ISM-ACES. (CR-2020-015)	Documentation	No impact to systems.
3	Changed RAW-FISA to RAWFISA. (CR-2020-007)	Documentation	No impact to systems.

B.3 - V2019-SEP Change Summary

Significant drivers for version 2019-SEP include:

- Technical Integration Committee Next Generation (TIC NG)

[Table 77](#) summarizes the changes made to this technical specification from version 2019-MARr2019-JUN to version 2019-SEP.

Table 77 - V2019-SEP Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Modified rules for tokens in the @fineAccessControls attribute to support hierarchical SCIs. (CR-2019-016).	Documentation	Data generation and ingestion systems for entity attributes need to be updated to accommodate the changes. ICAM systems and software services need to be updated to accommodate the changes.
2	Remove special access logic rules for HCS. HCS now operates like other SCIs. (CR-2019-075)	Documentation	Data generation and ingestion systems for entity attributes need to be updated to accommodate the changes. ICAM systems and software services need to be updated to accommodate the changes.
3	Update chapters for consistency with other specifications. (CR-2019-100).	Documentation	No impact to systems.

B.4 - V2019-MARr2019-JUN Change Summary

Significant drivers for Version 2019-MARr2019-JUN include:

- Omission of RAW-FISA, part of 2018-NOV, from the 2019-MAR release.

[Table 78](#) summarizes the changes made to this technical specification from Version 2018-AUG to Version 2018-NOV.

Table 78 - V2019-MARr2019-JUN Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Restored RAW-FISA dissemination controls. (CR-2019-067).	Documentation	Data generation and ingestion systems need to be updated to accommodate the changes to dissemination controls.

B.5 - V2019-MAR Change Summary

Significant drivers for Version 2019-MAR include:

- Consolidation of security control related specifications.

[Table 79](#) summarizes the changes made to this technical specification from Version 2018-AUG to Version 2019-MAR.

Table 79 - V2019-MAR Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Incorporation of Need-To-Know access control encoding. (CR-2018-095)	Documentation	No impact to systems that already implemented the Need-to-Know access control encodings.
2	Updated documentation to use the specification framework. (CR-2018-126)	Documentation	No impact to systems.

B.6 - V2018-NOV Change Summary

Significant drivers for Version 2018-NOV include:

- Community Change Requests
- New dissemination control markings being added to the next version of the *IC Markings System Register and Manual* [\[9\]](#).

[Table 80](#) summarizes the changes made to this technical specification from Version 2018-AUG to Version 2018-NOV.

Table 80 - V2018-NOV Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Add access rules for the new RAW-FISA dissemination control (CR-2018-135).	Documentation	Data generation and ingestion systems need to be updated to accommodate the changes to dissemination controls.

B.7 - V2018-AUG Change Summary

Significant drivers for Version 2018-AUG include:

- Community Change Requests.

[Table 81](#) summarizes the changes made to this technical specification from Version 2017-APR to Version 2018-AUG.

Table 81 - V2018-AUG Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Correct error introduced to RSV in 2018-APR to align RSV with all prior versions and other controls systems in the UIAS Compartment be represented without hierarchy. (CR-2018-118)	Documentation	Data generation and ingestion systems need to be updated to accommodate the changes to SCI controls.

B.8 - V2018-APR Change Summary

Significant drivers for Version 2018-APR include:

- Updates to SCI Controls.

[Table 82](#) summarizes the changes made to this technical specification from Version 2017-JUL to Version 2018-APR.

Table 82 - V2018-APR Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Simplify the SCI controls section to be more dynamic and based on the CVE values. (CR-2017-143)	Documentation	Data generation and ingestion systems need to be updated to accommodate the changes to SCI controls.
2	Updated section on Understanding Access Control to more accurately represent all of the specifications that participate in access control decisions. (CR-2018-071)	Documentation	No impact to systems.

B.9 - V2017-JUL Change Summary

Significant drivers for Version 2017-JUL include:

- *IC Marking System Register and Manual* 31 December 2016^[9]

[Table 83](#) summarizes the changes made to this technical specification from Version 2016-SEP to Version 2017-JUL.

Table 83 - V2017-JUL Change History

#	Change	Artifacts Changed	Compatibility Notes
1	Moving ECRU and NONBOOK as subcompartments under SI and handling the removal of ENDSEAL (CR-2015-097)	Documentation	Data generation and ingestion systems need to be updated to accommodate the changes to SCI controls.
2	Added definitions for Dependencies and Inverse Dependencies (CR-2017-262)	Documentation	No impact to systems.

B.10 - V2016-DEC Change Summary

Significant drivers for 2016-DEC include:

- Updates to correct access control logic regarding releasability with 2PIs.

The following table summarizes the changes made to 2016-SEP in developing 2016-DEC.

Table 84 - Data Encoding Specification V2016-DEC Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Updated the abstract and concrete sections for REL, DISPLAYONLY, EYES, and DSEN to appropriately account for when users or entities have multiple country of affiliation by using administrative organization to determine the appropriate country of affiliation (CR-2016-076)	ACES	Systems handling the impacted markings need to be updated.

B.11 - V2016-SEP Change Summary

Significant drivers for 2016-SEP include:

- Use the Tetragraph Taxonomy from the ISMCAT.CES^[28] specification for the breakdown of tetragraph membership.
- Updates to UIAS
- *IC Marking System Register and Manual* 24 December 2015^[9]

The following table summarizes the changes made to 2015-AUG in developing 2016-SEP.

Table 85 - Data Encoding Specification V2016-SEP Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Updated REL and DISPLAYONLY to refer to Tetragraph Taxonomy (ISMCAT) for tetragraph membership information (CR-2015-092, CR-2016-015)	ACES	Systems handling the impacted markings need to be updated.
2	Updated UIAS Annex to deal with the new handlingControls attribute for non-person entities. (CR-2015-037)	Documentation	Systems making access control decisions will need to be updated to support the new access/handling logic.
3	Remove HCS-O subcompartment logic (CR-2016-040)	Documentation	Systems making access control decisions will need to be updated to understand that HCS-O-XXX is no longer supported.
4	Administrative edits (CR-2016-007)	Documentation	No impact to systems.
5	Removed KDK and moved KDK subs under TK (CR-2016-024)	ACES	Systems making access control decisions will need to be updated to understand that KDK subs are now under TK and that KDK has been removed.
6	Update applicability section to reflect a requirement to comply with Law/Policy (CR-2016-063)	Documentation	Implementers must verify that they are complying with applicable laws and policies.

B.12 - V2015-AUG Change Summary

Significant drivers for 2015-AUG include:

- Community Change Requests
- Alignment with December 2014 IC Marking System Register and Manual^[10]

The following table summarizes the changes made to 2014-DEC in developing 2015-AUG.

Table 86 - Data Encoding Specification V2015-AUG Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Changed EYES to be limited to one or more of the Five Eyes Country Trigraphs	ACES	Systems handling the impacted markings need to be updated.
2	Provide access control of FISA to at least same level as FOUO	ACES	Systems handling the impacted markings need to be updated.

#	Change	Artifacts changed	Compatibility Notes
3	Corrected attribute for Non-IC controls in the UIAS appendix from ism:disseminationControls to ism:nonICmarkings.	ACES	Systems handling the impacted markings need to be updated.

B.13 - V2014-DEC Change Summary

Significant drivers for 2014-DEC include:

- December 2014 Intelligence Community Markings System Register and Manual^[10].
- Second Party Integrees requirements for Flow Control for originatingNetwork and issuingCertificate Authority.

The following table summarizes the changes made to V2 in developing 2014-DEC.

Table 87 - Data Encoding Specification V2014-DEC Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Changed DESVersion to represent the year and month of release. Also allowed for extension of specification by adding a '-' followed by a string to denote a custom implementation.	ACES	Systems referencing the version number need to handle the new format.
2	Updated NATO information to reflect NATO is treated as a read on and not a classification.	ACES	Systems handling the impacted markings need to be updated.
3	Updated to reflect treatment of SSI in the IC.	ACES	Systems handling the impacted markings need to be updated.
4	Updated to reflect treatment of SBU/SBU-NF in the IC.	ACES	Systems handling the impacted markings need to be updated.
5	Added Flow control for originatingNetwork and issuingCertificateAuthority.	ACES	All Systems making access control decisions MUST be updated to account for Flow control issues. If your trust chain includes anything other than ICPKI OR any system you return data to trusts anything other than ICPKI this is an import change for your system.
6	Handle NATO access as a read-on.	ACES	All Systems making access control decisions MUST be updated to account for this change.

#	Change	Artifacts changed	Compatibility Notes
7	Added markings FGI Protected, FGI Open NATO to show they do not impact an access control decision.	ACES	Systems handling the impacted markings need to be updated.
8	Added non-IC dissemination controls LIMDIS, EXDIS, NODIS, LES, LES-NF, NNPI, ACCM.	ACES	Systems handling the impacted markings need to be updated.

B.14 - V2 Change Summary

Significant drivers for Version 2 include:

- Additional SCI controls were required.
- Several markings were determined to not impact Access Control.
- UIAS.XML^[37] Standardized on Fine Access Control CVE for values.

The following table summarizes the changes made to V1 in developing V2.

Table 88 - Data Encoding Specification V2 Change Summary

#	Change	Artifacts changed	Compatibility Notes
1	Updated Five Eyes clearance level data to include CONFIDENTIAL as a minimum, and removed U from UIAS.XML ^[37] Attribute.	ACES	Systems handling 'R' data need to be updated to reflect this change.
2	Updated to align with Fine Access Control CVE.	ACES	Systems working with UIAS.XML ^[37] should be updated.
3	Added markings RS, FISA, IMC, and TFNI to show they do not impact an access control decision.	ACES	Systems handling the impacted markings need to be updated.

Appendix C Mapping ISM and UIAS Access & Flow

C.1 - Introduction

This appendix discusses the relationship of ISM.XML^[27] attributes on data objects to the entity attributes expressed in UIAS.XML^[37] for the purpose of access control. In the Access section, a document with the markings in the ISM.XML^[27] Attributes column **MUST** have all of the corresponding UIAS.XML^[37] attributes for access to be granted. Specifically, it gives an exact value-to-value mapping between the two specifications. This mapping is used for both Access, AC-3, and Flow AC-4, control purposes. For Access, the entity being evaluated is the “final” consumer, specifically the “user” who initiated a request. For Flow control purposes, the entity being evaluated would be the network or system in the “chain” between the final consumer and the user. Different architectures **MAY** require the immediate adjacent node to be the flow control or **MAY** require every node to be accounted for.

C.2 - Classification

This section describes the mapping of UIAS.XML^[37] clearance to the associated ISM.XML^[27] attributes and values sufficient for access.

C.2.1 - General Physical Rules

This section define physical mappings and rules that apply generally for access to ISM.XML^[27] documents.

C.2.1.1 - Non-USA Country Affiliation Access

This section describes the exact value mapping for access by a PE whose country affiliation does not contain **@USA** **or** whose organizational affiliation is not in *CVE Encoding Specification for US Agency Acronyms* (USAgency.CES^[38]).

Access to ISM.XML^[27] documents by an entity whose country affiliation does not contain USA, or whose organizational affiliation is not in *CVE Encoding Specification for US Agency Acronyms* (USAgency.CES^[38]), requires that:

1. The data **MUST** have a foreign disclosure and release marking of either REL TO, EYES or DISPLAY ONLY, **and**
2. The PE's attributes **MUST** match the document's ISM.XML^[27] attributes such that:
 - If **"REL"**, the PE **MUST** satisfy the requirements of [Section C.7.8 - Authorized For Release To \(REL\)](#).
 - If **"EYES"**, the PE **MUST** satisfy the requirements of [Section C.7.10 - Eyes Only \(EYES\)](#).
 - If **"DISPLAYONLY"**, the PE **MUST** satisfy the requirements of [Section C.7.14 - Authorized For Display But Not Release To \(DISPLAYONLY\)](#).

For the ISM.ACES abstract person requirements that match the attributes in the paragraph above, see [Section 2.2.4 - Non-USA Country Affiliation Access](#).

C.2.2 - Classification

This section describes the exact value mapping when the classification of the data asset is not a JOINT resource (i.e. `@ism:joint="true"` is not present). For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.1.1 - Classification](#).

Table 89 - US Classification

ISM Attributes	UIAS Attributes
<code>@ism:classification="TS"</code>	<code>clearance</code> contains "TS"
<code>@ism:classification="S"</code>	<code>clearance</code> contains one of "S", "TS"
<code>@ism:classification="C"</code>	<code>clearance</code> contains one of "C", "S", "TS"
<code>@ism:classification="R"</code>	<code>clearance</code> contains one of "R", "C", "S", "TS"
<code>@ism:classification="U"</code>	<code>digitalIdentifier</code> is present

C.2.3 - JOINT Classification

This section describes the exact value mapping when the classification of the data asset is a JOINT partner classification. For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.1.2 - JOINT Classification](#).

NOTE: "[LIST]" in the following table is used to represent the values of the `@ism:ownerProducer` attribute.

For the purposes of this section, the expression "[FullyExpandedList]" refers to the list of countries that results from expanding the member countries of any tetragraphs in "[LIST]" combined with the countries if any in "[LIST]". The expansion of the Tetragraphs MUST be done by referencing the current ISMCAT.CES^[28]. The concept of decomposability referenced in ISMCAT.CES^[28] is not relevant to access control. All Tetragraphs are able to be expanded to their member countries for the purpose of access control.

JOINT Classification

Table 90 - JOINT Classification

ISM Attributes	UIAS Attributes
@ism:ownerProducer="[LIST]", @ism:joint="true"	Requires: <ul style="list-style-type: none"> • At least one of countryOfAffiliation exists in "[FullyExpandedList]". • clearance is "TS" • One of <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • adminOrganization prefix before " _ " exists in "[FullyExpandedList]"
@ism:ownerProducer="[LIST]", @ism:joint="true"	Requires: <ul style="list-style-type: none"> • At least one of countryOfAffiliation exists in "[FullyExpandedList]" • clearance contains one of "S", "TS" • One of <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • adminOrganization prefix before " _ " exists in "[FullyExpandedList]"
@ism:ownerProducer="[LIST]", @ism:joint="true"	Requires: <ul style="list-style-type: none"> • At least one of countryOfAffiliation exists in "[FullyExpandedList]" • clearance contains one of "C", "S", "TS" • One of <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • adminOrganization prefix before " _ " exists in "[FullyExpandedList]"
@ism:ownerProducer="[LIST]", @ism:joint="true"	digitalIdentifier is present

C.2.4 - NATO Classification

This section describes the exact value mapping when the classification of the data asset is a NATO classification. For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.1.3 - NATO Classification](#).

Table 91 - NATO Classification

ISM Attributes	UIAS Attributes
@ism:ownerProducer="NATO", @ism:classification="TS"	fineAccessControls contains "NATO-TS".
@ism:ownerProducer contains but does not equal "NATO", @ism:highWaterNATO="TS"	fineAccessControls contains "NATO-TS".
@ism:ownerProducer="NATO", @ism:classification="S"	fineAccessControls contains "NATO-S" or "NATO-TS".
@ism:ownerProducer contains but does not equal "NATO", @ism:highWaterNATO="S"	fineAccessControls contains "NATO-S" or "NATO-TS".
@ism:ownerProducer="NATO", @ism:classification="C"	fineAccessControls contains "NATO-C", "NATO-S" or "NATO-TS"..
@ism:ownerProducer contains but does not equal "NATO", @ism:highWaterNATO="C"	fineAccessControls contains "NATO-C", "NATO-S" or "NATO-TS"..
@ism:ownerProducer="NATO", @ism:classification="R"	fineAccessControls contains "NATO-R", "NATO-C", "NATO-S" or "NATO-TS"..
@ism:ownerProducer contains but does not equal "NATO", @ism:highWaterNATO="R"	fineAccessControls contains "NATO-R", "NATO-C", "NATO-S" or "NATO-TS"..
@ism:ownerProducer="NATO", @ism:classification="U"	digitalIdentifier is present
@ism:ownerProducer contains but does not equal "NATO", @ism:highWaterNATO="U"	digitalIdentifier is present

C.2.5 - NATO NAC Classification

This section describes the exact value mapping when the classification of the data asset is a NATO NAC classification. For the purposes of this section the expression "[NC]" refers to the NAC as encoded for use in ISM.XML^[27]. For example NATO/Partnership for Peace would be Peace "NATO:Partnership_for_Peace". For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.1.4 - NATO NAC Classification](#).



Note

A NATO NAC MAY extend the country affiliation allowed for access beyond NATO. However that expansion would be on a NAC by NAC basis and would require verifying with the NAC owners for who the additional countries are.

Table 92 - NATO NAC Classification

ISM Attributes	UIAS Attributes
@ism:ownerProducer="NATO:[NC]", @ism:classification="TS"	fineAccessControls contains "NATO-TS".

ISM Attributes	UIAS Attributes
@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="TS"	fineAccessControls contains "NATO-TS".
@ism:ownerProducer="NATO:[NC]", @ism:classification="S"	fineAccessControls contains "NATO-S" or "NATO-TS".
@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="S"	fineAccessControls contains "NATO-S" or "NATO-TS".
@ism:ownerProducer="NATO:[NC]", @ism:classification="C"	fineAccessControls contains "NATO-C", "NATO-S" or "NATO-TS".
@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="C"	fineAccessControls contains "NATO-C", "NATO-S" or "NATO-TS".
@ism:ownerProducer="NATO:[NC]", @ism:classification="R"	fineAccessControls contains "NATO-R", "NATO-C", "NATO-S" or "NATO-TS".
@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="R"	fineAccessControls contains "NATO-R", "NATO-C", "NATO-S" or "NATO-TS".
@ism:ownerProducer="NATO:[NC]", @ism:classification="U"	digitalIdentifier is present.
@ism:ownerProducer contains but does not equal "NATO:[NC]", @ism:highWaterNATO="U"	digitalIdentifier is present.

C.3 - SCI Controls

This section describes the mapping of SCI control related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access consistent with the IC Markings System Register specific to ARH in the IC Markings^[9].



Warning

These instructions only apply to documents using @ism:SCIcontrols where the values are contained in the ISM.XML^[27] CVE "CEnumISMSCIControls". Values not in that CVE MAY Require additional user and system accreditation – contact the program manager for guidance.



Note

For Values not in ISM.XML^[27] CVE "CEnumISMSCIControls" contact the Specification team for guidance.

For the UIAS.XML^[37] attributes that implement the abstract person and NPE requirements in the table below, see [Section 5.2 - SCI Controls](#).

Table 93 - SCI Controls

ISM Attributes	Person or NPE attributes sufficient for access
@ism:SCIcontrols contains one or more tokens	For every token in @ism:SCIcontrols, the person or non-person entity's fineAccessControl attribute must contain that value.

C.4 - Special Access Programs

This section is meant to describe the physical mapping of SAP control related data attributes to a user's/person's attributes or a NPE's accreditation that are determined to be sufficient for access. However, since the SAP controls are all unpublished and cannot appear in either the ISM.XML^[27] CVENumISMSAR controlled vocabulary or the FAC.CES^[7] CVENumFineAccessControlType controlled vocabulary, detailed guidance regarding the actual SAP values cannot be provided in this specification. Contact the program manager for guidance on how to adapt ISM.XML^[27] and FAC.CES^[7] for unpublished SAPs that a system is authorized to process.

Detailed physical logic is provided below, both for SAPs that only have a single read-on **and** for DOD and potentially other agencies' SAPs that have different read-on levels for different classification levels. These rules are based on following patterns of SAP values in the ISM.XML^[27] CVENumISMSAR controlled vocabulary and the FAC.CES^[7] CVENumFineAccessControlType controlled vocabulary (see [Section 5.3 - Special Access Programs](#)).




For SAPs that have different read-ons for different classification levels, the UIAS.XML^[37] @fineAccessControls attribute **MUST** contain denormalized values to facilitate automated access control:


- If a user is granted a TOP SECRET read-on to a hypothetical DOD SAP STORMY PETREL, the user **MUST** have all of the following values in @fineAccessControls :
 - "DOD:TS:DEMOSAP1"
 - "DOD:S:DEMOSAP1"
 - "DOD:C:DEMOSAP1".
- If a user is granted a SECRET read-on to a hypothetical DOD SAP STORMY PETREL, the user **MUST** have all of the following values in @fineAccessControls :
 - "DOD:S:DEMOSAP1"
 - "DOD:C:DEMOSAP1".
- If a user is granted a CONFIDENTIAL read-on to a hypothetical DOD SAP STORMY PETREL, the user **MUST** have the following value in @fineAccessControls :
 - "DOD:C:DEMOSAP1".

This means that automated access control systems only need to do a simple match of a SAP token to the values in an entity's `@fineAccessControls`. For example, if `@ism:SARIdentifier` contains the token "DOD:S:DEMOSAP1", then a PDP only needs to check that an entity's `@fineAccessControls` contains "DOD:S:DEMOSAP1". An entity's `@fineAccessControls` will contain "DOD:S:DEMOSAP1" if the entity is briefed into DEMOSAP1 at either the S or TS level.

For the abstract logic regarding access to SAP data, see [Section 5.3 - Special Access Programs](#).

Table 94 - Special Access Programs

ISM Attributes	UIAS Attributes
<code>@ism:SARIdentifier</code> contains a SAP token that does not include any required classification level.	<code>fineAccessControls</code> contains the SAP.  Warning Requires additional user and system accreditation – contact the program manager for guidance.
<code>@ism:SARIdentifier</code> contains a SAP token that includes a required classification level of TS.	<code>fineAccessControls</code> contains the SAP at the TS level. For SAP token = "OwningAgency:TS:SAPMarking": <ul style="list-style-type: none"> <code>fineAccessControls</code> = "OwningAgency:TS:SAPMarking".  Warning Requires additional user and system accreditation – contact the program manager for guidance.
<code>@ism:SARIdentifier</code> contains a SAP token that includes a required classification level of SECRET.	The user has been read into the SAP at the S level. For SAP token = "OwningAgency:S:SAPMarking": <ul style="list-style-type: none"> <code>fineAccessControls</code> = "OwningAgency:S:SAPMarking".  Warning Requires additional user and system accreditation – contact the program manager for guidance.

ISM Attributes	UIAS Attributes
@ism:SARIdentifier contains a SAP token that includes a required classification level of CONFIDENTIAL.	<p>The user has been read into the SAP at the C level. For SAP token = "OwningAgency:C:SAPMarking":</p> <ul style="list-style-type: none"> • fineAccessControls = "OwningAgency:C:SAPMarking" <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5 - AEA Controls

C.5.1 - Restricted Data (RD)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.1 - Restricted Data \(RD\)](#).

Table 95 - RD

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "RD"	clearance contains "Q"

C.5.2 - Critical Nuclear Weapons Design Information (CNWDI)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.2 - Critical Nuclear Weapon Design Information \(CNWDI\)](#).


Table 96 - RD-CNWDI

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "RD-CNWDI"	<p>fineAccessControls contains "CNWDI"</p> <p>clearance contains "Q"</p>

C.5.3 - RD-SIGMA 14

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.3 - RD-SIGMA 14](#).


Table 97 - RD-SG-14

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "RD-SG-14"	<p>clearance contains "Q"</p> <p>Requires SIGMA 14 read on, however those are not tracked in UIAS.XML^[37] yet so automated decision MAY not be possible.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5.4 - RD-SIGMA 15

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.4 - RD-SIGMA 15](#).


Table 98 - RD-SG-15

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "RD-SG-15"	<p>clearance contains "Q"</p> <p>Requires SIGMA 15 read on, however those are not tracked in UIAS.XML^[37] yet so automated decision MAY not be possible.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5.5 - RD-SIGMA 18

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.5 - RD-SIGMA 18](#).


Table 99 - RD-SG-18

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "RD-SG-18"	<p>clearance contains "Q"</p> <p>Requires SIGMA 18 read on, however those are not tracked in UIAS.XML^[37] yet so automated decision MAY not be possible.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5.6 - RD-SIGMA 20

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.6 - RD-SIGMA 20](#).


Table 100 - RD-SG-20

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "RD-SG-20"	<p>clearance contains "Q"</p> <p>Requires SIGMA 20 read on, however those are not tracked in UIAS.XML^[37] yet so automated decision MAY not be possible.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5.7 - Formerly Restricted Data (FRD)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.7 - Formerly Restricted Data \(FRD\)](#).


Table 101 - FRD

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "FRD"	<p>The presence of FRD does not impact an access control decision. It may impact further handling, use, and releasability decisions.</p> <div>  <p>Caution</p> <p>The presence of a SIGMA with FRD DOES impact Access Control.</p> </div>

C.5.8 - FRD-SIGMA 14

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.8 - FRD-SIGMA 14](#).


Table 102 - FRD-SG-14

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "FRD-SG-14"	<p>clearance contains "Q"</p> <p>Requires SIGMA 14 read on, however those are not tracked in UIAS.XML^[37] yet so automated decision MAY not be possible.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5.9 - FRD-SIGMA 15

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.9 - FRD-SIGMA 15](#).


Table 103 - FRD-SG-15

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "FRD-SG-15"	<p>clearance contains "Q"</p> <p>Requires SIGMA 15 read on, however those are not tracked in UIAS.XML^[37] yet so automated decision MAY not be possible.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5.10 - FRD-SIGMA 18

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.10 - FRD-SIGMA 18](#).


Table 104 - FRD-SG-18

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "FRD-SG-18"	<p>clearance contains "Q"</p> <p>Requires SIGMA 18 read on, however those are not tracked in UIAS.XML^[37] yet so automated decision MAY not be possible.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5.11 - FRD-SIGMA 20

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.11 - FRD-SIGMA 20](#).

Table 105 - FRD-SG-20

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "FRD-SG-20"	<p>clearance contains "Q"</p> <p>Requires SIGMA 20 read on, however those are not tracked in UIAS.XML^[37] yet so automated decision MAY not be possible.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.5.12 - DoD Unclassified Controlled Nuclear Information (DCNI)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.12 - DoD Unclassified Controlled Nuclear Information \(DCNI\)](#).

Table 106 - DCNI

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:atomicEnergyMarkings contains "DCNI" and</p> <p>@ism:disseminationControls does not contain "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE has:</p> <ul style="list-style-type: none"> BOTH of: <ul style="list-style-type: none"> dutyOrganization in "[USAgencyList]" AND adminOrganization in "[USAgencyList]" AND one of: <ul style="list-style-type: none"> dutyOrganization not "USA.SLT" OR dutyOrganization of "USA.SLT" and entityType contains one of "GOV", "MIL", "SVR", "SVC", "DEV", "NET" (i.e., contractors are not authorized). <p>The NPE MUST have handlingControls containing "DCNI".</p>

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:atomicEnergyMarkings contains "DCNI" and</p> <p>@ism:disseminationControls contains "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE or NPE MUST meet:</p> <ul style="list-style-type: none"> • If "REL", the entity MUST satisfy the requirements of Section C.7.8 - Authorized For Release To (REL). • If "EYES", the entity MUST satisfy the requirements of Section C.7.10 - Eyes Only (EYES). • If "DISPLAYONLY", the entity MUST satisfy the requirements of Section C.7.14 - Authorized For Display But Not Release To (DISPLAYONLY).

C.5.13 - DoE Unclassified Controlled Nuclear Information (UCNI)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.13 - DoE Unclassified Controlled Nuclear Information \(UCNI\)](#).

Table 107 - UCNI

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:atomicEnergyMarkings contains "UCNI" and</p> <p>@ism:disseminationControls does not contain "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE has:</p> <ul style="list-style-type: none"> • BOTH of: <ul style="list-style-type: none"> • dutyOrganization in "[USAgencyList]" AND • adminOrganization in "[USAgencyList]" • AND one of: <ul style="list-style-type: none"> • dutyOrganization not "USA.SLT" OR • dutyOrganization of "USA.SLT" and entityType contains one of "GOV", "MIL", "SVR", "SVC", "DEV", "NET" (i.e., contractors are not authorized). <p>The NPE MUST have handlingControls containing "UCNI".</p>

ISM Attributes	Person or NPE attributes sufficient for access
<p>@ism:atomicEnergyMarkings contains "UCNI" and</p> <p>@ism:disseminationControls contains "REL", "EYES" or "DISPLAYONLY"</p>	<p>The PE or NPE MUST meet:</p> <ul style="list-style-type: none"> • If "REL", the entity MUST satisfy the requirements of Section C.7.8 - Authorized For Release To (REL). • If "EYES", the entity MUST satisfy the requirements of Section C.7.10 - Eyes Only (EYES). • If "DISPLAYONLY", the entity MUST satisfy the requirements of Section C.7.14 - Authorized For Display But Not Release To (DISPLAYONLY).

C.5.14 - Transclassified Foreign Nuclear Information (TFNI)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.4.14 - Transclassified Foreign Nuclear Information \(TFNI\)](#).

Table 108 - TFNI

ISM Attributes	UIAS Attributes
@ism:atomicEnergyMarkings contains "TFNI"	The presence of TFNI does not impact an access control decision. It may impact further handling, use, and releasability decisions.

C.6 - Foreign Government Information Markings


This section describes the exact value mapping between the @ism:FGISourceProtected, @ism:FGISourceOpen attributes and the appropriate UIAS.XML^[37] attributes.

C.6.1 - FGI Protected

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.5.1 - FGI Protected](#).

Table 109 - FGI Protected

ISM Attributes	UIAS Attributes
@ism:FGISourceProtected equals "FGI"	The presence of FGI protected does not impact an access control decision. It may impact further handling, use, and releasability decisions.

ISM Attributes	UIAS Attributes
@ism:FGISourceProtected does NOT equal "FGI"	<p>The Access decision logic for FGI is not yet codified in this ACES. The classification and other appropriate markings when revealing the FGI country MUST be determined by the data owner.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.6.2 - FGI Open NATO

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.5.2 - FGI Open NATO](#).

Table 110 - FGI Open

ISM Attributes	UIAS Attributes
@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-TS"	fineAccessControls contains "NATO-TS".
@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-S"	fineAccessControls contains "NATO-S" or "NATO-TS".
@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-C"	fineAccessControls contains "NATO-C", "NATO-S" or "NATO-TS".
@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-R"	fineAccessControls contains "NATO-R", "NATO-C", "NATO-S" or "NATO-TS".
@ism:FGISourceOpen contains "NATO" and @ism:highWaterNATO="NATO-U"	digitalIdentifier is present.
@ism:FGISourceOpen does NOT contain "NATO"	The presence of FGI open without NATO does not impact an access control decision. It may impact further handling, use, and releasability decisions.


C.7 - Dissemination Controls

This section describes the exact value mapping between the @ism:disseminationControls attribute and the appropriate UIAS.XML^[37] attributes.

C.7.1 - Risk Sensitive (RS)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.1 - Risk Sensitive \(RS\)](#).

Table 111 - RS

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "RS"	<p>For person entities, the presence of RS does not impact an access control decision.</p> <p>For NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "RS"</p> <div>  <div> <p>Note</p> <p>It may impact further handling, use, and releasability decisions. Risk Sensitive has a portion marking of RS but a banner marking of RSEN.</p> </div> </div>

C.7.2 - For Official Use Only (FOUO)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.2 - For Official Use Only \(FOUO\)](#).

Table 112 - FOUO

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "FOUO" and does not contain "REL", "EYES" or "DISPLAYONLY"	<p>For PE,</p> <ul style="list-style-type: none"> The value of dutyOrganization MUST be found in "[USAgencyList]" <p>AND</p> <ul style="list-style-type: none"> The value of adminOrganization MUST be found in "[USAgencyList]" <p>For NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "FOUO".</p>

ISM Attributes	Person or NPE attributes sufficient for access
@ism:disseminationControls contains "FOUO" and contains "REL", "EYES" or "DISPLAYONLY"	<p>The PE or NPE MUST meet:</p> <ul style="list-style-type: none"> • If "REL", the entity MUST satisfy the requirements of Section C.7.8 - Authorized For Release To (REL). • If "EYES", the entity MUST satisfy the requirements of Section C.7.10 - Eyes Only (EYES). • If "DISPLAYONLY", the entity MUST satisfy the requirements of Section C.7.14 - Authorized For Display But Not Release To (DISPLAYONLY).

C.7.3 - Originator Controlled (OC)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.3 - Originator Controlled \(OC\)](#).

Originator Controlled data requires the use of a "OC-NTK" Need-To-Know profile for access control determinations. The Need-To-Know profile of "OC-NTK" details the agencies permitted access by the data's originating agency as expressed in this ACES. There is no direct ISM.XML^[27] to UIAS.XML^[37] mapping. Please see the [Section C.10.7 - Mapping ORCON to UIAS](#) for guidance on access control decisions related to OC and for the UIAS.XML^[37] mapping.

Table 113 - OC

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "OC" and not "OC-USGOV"	See Section C.10.7 - Mapping ORCON to UIAS for interpreting the required OC-NTK statement.
@ism:disseminationControls contains "OC" and "OC-USGOV"	See Section C.7.4 - Originator Controlled US Government (OC-USGOV) rules.

C.7.4 - Originator Controlled US Government (OC-USGOV)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.4 - Originator Controlled US Government \(OC-USGOV\)](#).

For the purposes of this section the expression "[USGovList]" refers to the list of organizations in the USGOV Agency Acronym List with namespace urn:us:gov:ic:cvenum:usgovagency:agencyacronym.

Table 114 - OC-USGOV

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "OC" and "OC-USGOV"	dutyOrganization exists in "[USGovList]" or in the Need-To-Know metadata block specified on the document as an @ntk:qualifier="originator" or @ntk:qualifier="authorizedDissem" organization.

C.7.5 - Controlled Imagery (IMC)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.5 - Controlled Imagery \(IMC\)](#).

Table 115 - IMC

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "IMC"	<p>For person entities, the presence of IMC does not impact an access control decision. It may impact further handling, use, and releasability decisions.</p> <p>For NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "IMC"</p>

C.7.6 - Not Releasable To Foreign Nationals (NF)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.6 - Not Releasable To Foreign Nationals \(NF\)](#).

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.



Warning

Entities eligible for NF data MAY still be ineligible to receive it based on flow control restrictions, see [Appendix D - Mapping ISM and UIAS Flow Control](#)

Table 116 - NF

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "NF"	<p>If a person entity, MUST satisfy all of the following:</p> <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • countryOfAffiliation contains "USA" <p>If NPE, MUST have UIAS.XML^[37] attribute handlingControls containing either "NF" or "USONLY" or "REL".</p>

C.7.7 - Caution-Proprietary Information Involved (PR)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.7 - Caution-Proprietary Information Involved \(PR\)](#).

PROPIN requires the use of the Need-To-Know metadata profile "PROPIN-NTK" which details the users permitted access by the data's owner. There is no direct ISM attribute to UIAS.XML^[37] mapping. Please see the [Section C.10.9 - Mapping PROPIN to UIAS](#) specification for guidance on access control decisions related to PROPIN.

Table 117 - PR

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "PR"	See the Section C.10.9 - Mapping PROPIN to UIAS section for guidance on access control decisions related to PROPIN.

C.7.8 - Authorized For Release To (REL)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.8 - Authorized For Release To \(REL\)](#).

For the purposes of this section, the expression "[LIST]" refers to a subset list of countries within the ISMCAT.CES^[28] CVE "RelTo" with namespace urn:us:gov:ic:cvenum:ismcat:relto.

For the purposes of this section, the expression "[FullyExpandedList]" refers to the list of countries that results from expanding the member countries of any tetragraphs in "[LIST]" combined with the countries if any in "[LIST]". The expansion of the Tetragraphs MUST be done by referencing the current ISMCAT.CES^[28]. The concept of decomposability referenced in ISMCAT.CES^[28] is not relevant to access control. All Tetragraphs are able to be expanded to their member countries for the purpose of access control.



Note

Tetragraph values whose membership is not countries but a descriptive text outlining membership which is not currently machine processable should be ignored for access control decisions.



Warning

Entities eligible for REL data MAY still be ineligible to receive it based on flow control restrictions, see [Appendix D - Mapping ISM and UIAS Flow Control](#)


Table 118 - REL

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "REL", @ism:releasableTo="[LIST]"	<p>Requires:</p> <ul style="list-style-type: none"> At least one of countryOfAffiliation MUST exist in "[FullyExpandedList]". One of <ul style="list-style-type: none"> adminOrganization exists in "[USAgencyList]" adminOrganization prefix before "_" exists in "[FullyExpandedList]" <p>AND</p> <p>For NPEs, MUST have UIAS.XML^[37] attribute handlingControls with "[REL]" or meet <i>one of</i> the following criteria:</p> <ul style="list-style-type: none"> UIAS.XML^[37] attribute handlingControls with "REL_TEYE" and "[FullyExpandedList]" containing no less than "USA", "AUS", and "GBR" UIAS.XML^[37] attribute handlingControls with "REL_ACGU" and "[FullyExpandedList]" containing no less than "USA", "AUS", "CAN", and "GBR" UIAS.XML^[37] attribute handlingControls with "REL_FVEY" and "[FullyExpandedList]" containing no less than "USA", "AUS", "CAN", "GBR", and "NZL" UIAS.XML^[37] attribute handlingControls with "USONLY"

C.7.9 - Releasable By Information Disclosure Official (RELIDO)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.9 - Releasable By Information Disclosure Official \(RELIDO\)](#).

Table 119 - RELIDO

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "RELIDO"	<p>The presence of RELIDO does not impact an access control decision. It may impact further handling, use, and releasability decisions.</p> <div>  <p>Warning</p> <p>RELIDO is does not allow for any foreign distribution by itself. REL and DISPLAYONLY are the only marks that enable foreign distribution.</p> </div>

C.7.10 - Eyes Only (EYES)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.10 - Eyes Only \(EYES\)](#).

For the purposes of this section, the expression "[LIST]" refers to the list of the Five Eyes Country Trigraphs within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto. The expression "[LIST]" MUST contain "USA" and one or more of the following: "AUS", "CAN", "GBR", or "NZL".

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.



Note

Tetragraph values whose membership is not countries but a descriptive text outlining membership which is not currently machine processable should be ignored for access control decisions.



Warning

Entities eligible for EYES data MAY still be ineligible to receive it based on flow control restrictions, see [Appendix D - Mapping ISM and UIAS Flow Control](#)

Table 120 - EYES

ISM Attributes	UIAS Attributes
<p>@ism:disseminationControls contains "EYES", @ism:releasableTo="[LIST]"</p>	<p>Requires:</p> <ul style="list-style-type: none"> • At least one of countryOfAffiliation MUST exist in "[LIST]". • One of <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • adminOrganization prefix before " " exists in "[LIST]" <p>AND</p> <p>For NPEs, MUST have UIAS.XML^[37] attribute handlingControls with "REL" or meet <i>one</i> of the following criteria:</p> <ul style="list-style-type: none"> • UIAS.XML^[37] attribute handlingControls with "REL_TEYE" and "[LIST]" containing no less than "USA", "AUS", and "GBR" • UIAS.XML^[37] attribute handlingControls with "REL_ACGU" and "[LIST]" containing no less than "USA", "AUS", "CAN", and "GBR" • UIAS.XML^[37] attribute handlingControls with "REL_FVEY" and "[LIST]" containing no less than "USA", "AUS", "CAN", "GBR", and "NZL" • UIAS.XML^[37] attribute handlingControls with "USONLY"

C.7.11 - DEA Sensitive (DSEN)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.11 - DEA Sensitive \(DSEN\)](#).

Table 121 - DSEN

ISM Attributes	UIAS Attributes
<p>@ism:disseminationControls contains "DSEN" and does not contain "REL", "EYES", or "DISPLAYONLY"</p>	<p>The person MUST meet:</p> <ul style="list-style-type: none"> One of: <ul style="list-style-type: none"> dutyOrganization not "USA.SLT" dutyOrganization of "USA.SLT" and entityType contains one of "GOV", "MIL", "SVR", "SVC", "DEV", "NET" (i.e., contractors are not authorized) <div data-bbox="922 646 1015 743"> </div> <p>Note</p> <p>UIAS does not track interim vs final clearances. It only has final clearances. So there is no need to have a special clearance check for classified DSEN.</p> <ul style="list-style-type: none"> AND all of: <ul style="list-style-type: none"> countryOfAffiliation contains "USA" adminOrganization exists in "[USAgencyList]" <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> The NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "DSEN"

ISM Attributes	UIAS Attributes
<p>@ism:disseminationControls contains "DSEN" and contains either "REL", "EYES", or "DISPLAYONLY"</p>	<p>The person or NPE MUST meet</p> <ul style="list-style-type: none"> One of: <ul style="list-style-type: none"> dutyOrganization not "USA.SLT" dutyOrganization of "USA.SLT" and entityType contains one of "GOV", "MIL", "SVR", "SVC", "DEV", "NET" (i.e., contractors are not authorized) <div data-bbox="922 583 1015 682"></div> <p>Note</p> <p>UIAS.XML^[37] does not track interim vs final clearances. It only has final clearances. So there is no need to have a special clearance check for classified DSEN.</p> <ul style="list-style-type: none"> AND any applicable <ul style="list-style-type: none"> If "REL", MUST satisfy the requirements of Table 118 If "EYES", MUST satisfy the requirements of Table 120 If "DISPLAYONLY", MUST satisfy the requirements of Table 124 <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> The NPE MUST have UIAS.XML^[37] attribute handlingControls containing "DSEN"

C.7.12 - RAWFISA

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.12 - Raw Foreign Intelligence Surveillance Act \(RAWFISA\)](#).

Table 122 - RAWFISA

ISM Attributes	UIAS Attributes
ism:disseminationControls contains "RAWFISA"	<p>For person entities, the presence of RAWFISA does not impact an access control decision. It may impact further handling, use, and releasability decisions.</p> <p>For NPE, MUST have UIAS.XML^[37] attribute handlingControls containing [RAWFISA]</p>

C.7.13 - Foreign Intelligence Surveillance Act (FISA)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.13 - Foreign Intelligence Surveillance Act \(FISA\)](#).

Table 123 - FISA

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "FISA" and @ism:classification equal "U"	<p>For person entities, Unclassified data marked for FISA dissemination SHOULD be treated as FOUO. See ISM.ACES UIAS entry Section C.7.2 - For Official Use Only (FOUO).</p> <p>AND</p> <p>For NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "FISA"</p>
@ism:disseminationControls contains "FISA" and @ism:classification NOT equal "U"	<p>For person entities, the presence of FISA, in classified data, does not impact an access control decision for person entities. It may impact further handling, use, and releasability decisions.</p> <p>For NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "FISA"</p>

C.7.14 - Authorized For Display But Not Release To (DISPLAYONLY)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.14 - Authorized For Display But Not Release To \(DISPLAYONLY\)](#).

For the purposes of this section the expression "[DLIST]" and "[RLIST]" refers to the list of countries within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto. For a breakdown of tetragraph values in either, please refer to the Tetragraph Taxonomy in the ISMCAT.CES^[28] specification.

For the purposes of this section the expression `<tag class="attvalue">[COMPLETE-LIST]</tag>` refers to the union of "[DLIST]" and "[RLIST]". If "[RLIST]" does not exist treat "[RLIST]" as an empty set.

For the purposes of this section, the expression "[FullyExpandedList]" refers to the list of countries that results from expanding the member countries of any tetragraphs in `<tag class="attvalue">[COMPLETE-LIST]</tag>` combined with the countries if any in `<tag class="attvalue">[COMPLETE-LIST]</tag>`. The expansion of the Tetragraphs MUST be done by referencing the current ISMCAT.CES^[28]. The concept of decomposability referenced in ISMCAT.CES^[28] is not relevant to access control. All Tetragraphs are able to be expanded to their member countries for the purpose of access control.



Note

Tetragraph values whose membership is not countries but a descriptive text outlining membership which is not currently machine processable should be ignored for access control decisions.



Warning

Entities eligible for DISPLAYONLY data MAY still be ineligible to receive it based on flow control restrictions, see [Appendix D - Mapping ISM and UIAS Flow Control](#)

Table 124 - DISPLAYONLY

ISM Attributes	UIAS Attributes
<p><code>@ism:disseminationControls</code> contains "DISPLAYONLY", <code>@ism:displayOnlyTo=" [LIST] "</code></p> <p>Optionally there may be <code>@ism:releasableTo=" [RLIST] "</code></p>	<p>The person meeting the following is granted viewing access, but not the ability to copy, duplicate, or further disseminate the resource in any way.</p> <ul style="list-style-type: none"> At least one of <code>countryOfAffiliation</code> MUST exist in "[FullyExpandedList]". One of <ul style="list-style-type: none"> <code>adminOrganization</code> exists in "[USAgencyList]" <code>adminOrganization</code> prefix before " " exists in "[FullyExpandedList]" <p>The person meeting the following is not impacted by the presence of DISPLAYONLY in any way as they are a US citizen working for the US, Display Only is only a limitation on partners.</p> <ul style="list-style-type: none"> At least one of <code>countryOfAffiliation</code> MUST be "USA". AND <code>adminOrganization</code> exists in "[USAgencyList]" <p>The NPE MUST meet:</p> <ul style="list-style-type: none"> UIAS.XML^[37] attribute <code>handlingControls</code> containing either "DISPLAYONLY" or "USONLY". <div data-bbox="816 1423 912 1520"> </div> <p>Warning</p> <p>Access granted by the presence of at least one of <code>countryOfAffiliation</code> in the <code>@ism:releasableTo</code> attribute include and exceed that granted by Display Only To and as such the restrictions mentioned here would be superseded by the access granted by Releasable To or by <code>adminOrganization</code> exists in "[USAgencyList]".</p>

C.7.15 - Exempt from ICD-501 Discovery

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.6.15 - EXEMPT FROM ICD-501 DISCOVERY](#).

Table 125 - FISA

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "EXEMPT_FROM_ICD501_DISCOVERY"	When person or NPE entities submit a search to discover information collected and/or analysis produced in accordance with <i>Discovery and Dissemination or Retrieval of Information within the Intelligence Community</i> ^[17] , the search systems should not return any documents with @ism:disseminationControls contains "EXEMPT_FROM_ICD501_DISCOVERY".

C.8 - Non-IC Dissemination Controls

This section describes the exact value mapping between the @ism:nonICmarkings attribute and the appropriate UIAS.XML^[37] attributes.

C.8.1 - Limited Distribution (LIMDIS)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.1 - Limited Distribution \(LIMDIS\)](#).

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.

Table 126 - LIMDIS

ISM Attributes	UIAS Attributes
@ism:disseminationControls contains "DS" and does not contain "REL", "EYES", or "DISPLAYONLY"	<p>Requires:</p> <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • dutyOrganization exists in "[USGovList]" • countryOfAffiliation contains "USA" <p>AND</p> <p>For NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "DS"</p>

ISM Attributes	UIAS Attributes
<p>@ism:disseminationControls contains "DS" and contains "REL", "EYES", or "DISPLAYONLY"</p>	<p>Requires:</p> <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • dutyOrganization exists in "[USGovList]" <p>AND</p> <p>For NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "DS"</p> <p>AND</p> <ul style="list-style-type: none"> • If "REL", MUST satisfy the requirements of Table 118 • If "EYES", MUST satisfy the requirements of Table 120 • If "DISPLAYONLY", MUST satisfy the requirements of Table 124

C.8.2 - Exclusive Distribution (EXDIS)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.2 - Exclusive Distribution \(EXDIS\)](#).

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.

Table 127 - EXDIS

ISM Attributes	UIAS Attributes
@ism:nonICmarkings contains "XD"	<p>Requires:</p> <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • dutyOrganization exists in "[USGovList]" and be one of the department or agency specified by the originator. • countryOfAffiliation contains "USA" <p>AND</p> <p>Satisfy the requirements specified in Section C.10.2 - Mapping EXDIS to UIAS for guidance on access control decisions related to EXDIS.</p>

C.8.3 - No Distribution (NODIS)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.3 - No Distribution \(NODIS\)](#).

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.

Table 128 - NODIS

ISM Attributes	UIAS Attributes
@ism:nonICmarkings contains "ND"	<p>Requires:</p> <ul style="list-style-type: none"> • adminOrganization exists in "[USAgencyList]" • Requires access by named individual. • countryOfAffiliation contains "USA" <p>AND</p> <p>Satisfy the requirements specified in the Section C.10.6 - Mapping NODIS to UIAS for guidance on access control decisions related to No Distribution (NODIS).</p>

C.8.4 - Sensitive But Unclassified (SBU)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.4 - Sensitive But Unclassified \(SBU\)](#).

Table 129 - SBU

ISM Attributes	Person or NPE attributes sufficient for access
@ism:atomicEnergyMarkings contains "SBU" and @ism:disseminationControls does not contain "REL", "EYES" or "DISPLAYONLY"	<p>A PE MUST meet ALL of:</p> <ul style="list-style-type: none"> • dutyOrganization in "[USAgencyList]" AND • adminOrganization in "[USAgencyList]" AND • dutyOrganization is not "USA.SLT". <p>An NPE MUST have UIAS.XML^[37] attribute handlingControls containing [SBU].</p>
@ism:atomicEnergyMarkings contains "SBU" and @ism:disseminationControls contains "REL", "EYES" or "DISPLAYONLY"	<p>A PE MUST meet:</p> <ul style="list-style-type: none"> • If "REL", the entity MUST satisfy the requirements of Section C.7.8 - Authorized For Release To (REL). • If "EYES", the entity MUST satisfy the requirements of Section C.7.10 - Eyes Only (EYES). • If "DISPLAYONLY", the entity MUST satisfy the requirements of Section C.7.14 - Authorized For Display But Not Release To (DISPLAYONLY). <p>An NPE MUST have UIAS.XML^[37] attribute handlingControls containing [SBU].</p>

C.8.5 - Sensitive But Unclassified NOFORN (SBU-NF)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.5 - Sensitive But Unclassified NOFORN \(SBU-NF\)](#).

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.

Table 130 - SBU-NF

ISM Attributes	UIAS Attributes
@ism:nonICmarkings contains "SBU-NF"	<p>A PE MUST meet ALL of:</p> <ul style="list-style-type: none"> • dutyOrganization exists in "[USAgencyList]" AND • dutyOrganization is not "USA.SLT" AND • adminOrganization exists in "[USAgencyList]" AND • countryOfAffiliation contains "USA". <p>An NPE MUST satisfy ALL of the following conditions:</p> <ul style="list-style-type: none"> • The UIAS.XML^[37] attribute handlingControls contains "SBU-NF". • The UIAS.XML^[37] attribute handlingControls contains either "NF" or "USONLY" or "REL".

C.8.6 - Law Enforcement Sensitive (LES)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.6 - Law Enforcement Sensitive \(LES\)](#).

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.

Table 131 - LES

ISM Attributes	UIAS Attributes
@ism:nonICmarkings contains "LES" and not "REL", "EYES", "DISPLAYONLY"	<p>adminOrganization MUST exist in "[USAgencyList]"</p> <p>AND</p> <p>An NPE MUST have UIAS.XML^[37] attribute handlingControls containing "LES"</p>

ISM Attributes	UIAS Attributes
@ism:nonICmarkings contains "LES" and at least one of "REL", "EYES", "DISPLAYONLY"	digitalIdentifier is present AND An NPE MUST have UIAS.XML ^[37] attribute handlingControls containing "LES"

C.8.7 - Law Enforcement Sensitive NOFORN (LES-NF)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.7 - Law Enforcement Sensitive NOFORN \(LES-NF\)](#).

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace urn:us:gov:ic:cvenum:usagency:agencyacronym.

Table 132 - LES-NF

ISM Attributes	UIAS Attributes
@ism:nonICmarkings contains "LES-NF"	Requires: <ul style="list-style-type: none"> countryOfAffiliation contains "USA" adminOrganization exists in "[USAgencyList]" AND An NPE MUST satisfy ALL of the following conditions: <ul style="list-style-type: none"> The UIAS.XML^[37] attribute handlingControls contains "LES" The UIAS.XML^[37] attribute handlingControls contains either "NF" or "USONLY" or "REL".

C.8.8 - Sensitive Security Information (SSI)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.8 - Sensitive Security Information \(SSI\)](#).


Table 133 - SSI

ISM Attributes	UIAS Attributes
@ism:nonICmarkings contains "SSI".	clearance contains one of "S", "TS" AND For NPE, MUST have UIAS.XML ^[37] attribute handlingControls containing "SSI"

C.8.9 - Naval Nuclear Propulsion Information (NNPI)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.9 - Naval Nuclear Propulsion Information \(NNPI\)](#).


Table 134 - NNPI

ISM Attributes	UIAS Attributes
@ism:nonICmarkings contains "NNPI"	<p>The Access decision logic for NNPI is not codified in this ACES.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.8.10 - Alternate Compensatory Control Measure (ACCM)

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.7.10 - Alternate Compensatory Control Measure \(ACCM\)](#).

Table 135 - ACCM

ISM Attributes	UIAS Attributes
Not Supported in ISM.XML ^[27] without extension. Work with standards team if this is required.	<p>The Access decision logic for ACCM is not codified in this ACES.</p> <div>  <p>Warning</p> <p>Requires additional user and system accreditation – contact the program manager for guidance.</p> </div>

C.9 - NATO Controls

C.9.1 - ATOMAL

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.8.1 - ATOMAL](#).

Table 136 - ATOMAL

ISM Attributes	UIAS Attributes
@ism:nonUSControls contains "NATO-ATOMAL"	fineAccessControls contains "NATO-ATOMAL"

C.9.2 - BALK

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.8.2 - BALK](#).

Table 137 - BALK

ISM Attributes	UIAS Attributes
@ism:nonUSControls contains "NATO-BALK"	fineAccessControls contains "NATO-BALK"

C.9.3 - BOHEMIA

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 5.8.3 - BOHEMIA](#).

Table 138 - BOHEMIA

ISM Attributes	UIAS Attributes
@ism:nonUSControls contains "NATO-BOHEMIA"	fineAccessControls contains "NATO-BOHEMIA"

C.10 - Mapping Need-To-Know Access Profiles to UIAS

C.10.1 - Introduction

This section discusses the relationship of Need-To-Know Access Profiles on data objects to the entity attributes expressed in UIAS.XML^[37] for the purpose of access control. In the Access section, a document with the markings in the Need-To-Know column must have all of the corresponding UIAS.XML^[37] Attributes for access to be granted. Specifically, it gives an exact value-to-value mapping between the two specifications. This mapping is used for both Access, AC-3, and Flow, AC-4, control purposes. For Access, the entity being evaluated is the *final* consumer, specifically the *user* who initiated a request. For Flow control purposes, the entity being

evaluated would be the network or system in the *chain* between the final consumer and the user. Different architectures MAY require the immediate adjacent node to be the flow control or MAY require every node to be accounted for.

C.10.2 - Mapping EXDIS to UIAS

This section discusses the relationship of EXDIS markings on data objects to the entity attributes expressed in UIAS.XML^[37]. The ISM.XML^[27] `@ism:nonICmarkings` value of "XD" requires an EXDIS access policy be present.

The following table provides a mapping from specific EXDIS Need-To-Know elements to concrete UIAS.XML^[37] attributes. The "[ORIG_AGENCY]" and "[DISSEM_AGENCY]" tokens are placeholder values; these placeholders stand for actual agency acronyms used in an EXDIS Need-To-Know assertion. There may be multiple `ntk:AccessProfileValue` elements listing agencies authorized for dissemination.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.2 - Exclusive Distribution](#).

Table 139 - EXDIS Access Control Mapping

ntk:AccessProfile	UIAS Attribute
<p>ntk:AccessPolicy contains the EXDIS URN</p> <pre><ntk:AccessPolicy>urn:us:gov:ic:aces:ntk:xd</ntk:AccessPolicy></pre>	<p>The person or NPE MUST meet at <i>least one</i> of these criteria:</p> <ol style="list-style-type: none">1. The person or NPE UIAS.XML^[37] attribute dutyOrganization matches "[ORIG_AGENCY]"2. The person or NPE UIAS.XML^[37] attribute dutyOrganization matches one of "[DISSEM_AGENCY]"
<p>ntk:ProfileDes contains the Agency Dissem URN</p> <pre><ntk:ProfileDes>urn:us:gov:ic:ntk:profile:agencydissem</ntk:ProfileDes></pre>	
<p>exactly one originator agency</p> <pre><ntk:AccessProfileValue ntk:qualifier="originator" ntk:vocabulary="organization:usa-agency" >[ORIG_AGENCY]</ntk:AccessProfileValue></pre>	
<p>zero to many dissemto agencies</p> <pre><ntk:AccessProfileValue ntk:qualifier="dissemto" ntk:vocabulary="organization:usa-agency" >[DISSEM_AGENCY]</ntk:AccessProfileValue></pre>	
<p>AND</p> <p>If NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "XD"</p>	

C.10.3 - Mapping ICO to UIAS

This section discusses the relationship of ICO constraint on data objects to the entity attributes expressed in the UIAS.XML^[37] specification. The following Access Control Mapping table provides a mapping from specific ICO elements to concrete UIAS.XML^[37] attributes.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.3 - Intelligence Community Only](#).

Table 140 - Restriction to IC Members

ntk:AccessProfile	UIAS Attributes
<p>ntk:AccessPolicy contains the ICO URN</p> <pre><ntk:AccessProfile ism:classification="U" ism:ownerProfile="USA"> <ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:ico </ntk:AccessPolicy> </ntk:AccessProfile></pre>	<p>The person or NPE UIAS.XML^[37] attribute isICMember MUST be "TRUE".</p>

C.10.4 - Mapping LICENSE to UIAS

This section discusses the relationship of LICENSE constraints on data objects to the entity attributes expressed in the UIAS.XML^[37] specification.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.4 - License](#).

Table 141 - LICENSE-NTK Access List



LICENSE-NTK	UIAS Attributes
<p>ntk:AccessPolicy contains the License URN</p> <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:license </ntk:AccessPolicy></pre> <p>ntk:ProfileDes contains the Data Sphere URN</p> <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:datasphere </ntk:ProfileDes></pre> <p>one to many licenses</p> <pre><ntk:AccessProfileValue ntk:vocabulary="datasphere:license" >[LICENSE]</ntk:AccessProfileValue></pre>	<p>The person or NPE MUST meet <i>all</i> of these criteria:</p> <ol style="list-style-type: none"> 1. If "osc1" is one of the "[LICENSE]" values, the entity's UIAS.XML^[37] attribute isICMember must be "TRUE". 2. The person or NPE MUST meet the requirements for <i>all</i> other license agreements as indicated by the set of "[LICENSE]" values.

C.10.5 - Mapping MN to UIAS

This section discusses the relationship of Mission Need constraints on data objects to the entity attributes expressed in the UIAS.XML^[37] specification. The following Access Control Mapping table provides a mapping from specific Mission Need elements to concrete UIAS.XML^[37] attributes. The **"[ISSUE]"** and **"[REGION]"** tokens are placeholder values; these placeholders stand for actual issues and regions used in a Mission Need Need-To-Know assertion.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.5 - Mission Need](#).

Table 142 - MN-NTK Access List

MN-NTK	UIAS Attributes
ntk:AccessPolicy contains the MN URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:mn </ntk:AccessPolicy></pre>	<p>The person or NPE MUST meet <i>both</i> the issue and region criteria:</p> <p>Issue Criteria. If Mission Need issues are listed in the Need-To-Know Access Profile, the UIAS.XML^[37] attribute topic MUST contain at least one of the listed "[ISSUE]" values.</p>
ntk:ProfileDes contains the Data Sphere URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:datasphere </ntk:ProfileDes></pre>	
zero to many MN issues <pre><ntk:AccessProfileValue ntk:vocabulary="datasphere:mn:issue" >[ISSUE]</ntk:AccessProfileValue></pre>	 <p>Note</p> <p>If no Mission Need issues are listed in the Need-To-Know metadata, there is no issue restriction.</p>
zero to many MN regions <pre><ntk:AccessProfileValue ntk:vocabulary="datasphere:mn:region" >[REGION]</ntk:AccessProfileValue></pre>	<p>Region Criteria. If Mission Need regions are listed in the Need-To-Know Access Profile, the UIAS attribute region MUST contain at least one of the listed "[REGION]" values.</p>  <p>Note</p> <p>If no Mission Need regions are listed in the Need-To-Know metadata there is no region restriction.</p>

C.10.6 - Mapping NODIS to UIAS

This section discusses the relationship of NODIS markings on data objects to the entity attributes expressed in UIAS.XML^[37] with the focus on the agency dissemination **ntk:ProfileDes** for data markings. The ISM.XML^[27] **@ism:nonICmarkings** value of "ND" requires an NODIS access policy be present.

The following Access Control Mapping table provides a mapping from specific NODIS Need-To-Know elements to concrete UIAS.XML^[37] attributes. The use of [TYPES] below is the notional place holder for actual vocabulary types defined in Need-To-Know metadata. There may be multiple **ntk:AccessProfileValue** elements listing groups or individuals authorized for dissemination.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.6 - No Distribution](#).

Table 143 - ND-NTK Access List

ND-NTK	UIAS Attributes
<p>ntk:AccessPolicy contains the NODIS URN</p> <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:nd </ntk:AccessPolicy></pre>	<p>The user or NPE MUST meet <i>at least one</i> of these criteria:</p>
<p>ntk:ProfileDes contains the Group & Individual URN</p> <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre>	<p>1. One or more IAA Service Provider Entitlement Management Service groups are listed in the NTK Access Profile and the entity's UIAS.XML^[37] group attribute contains at least one "[GRP_VALUE]" from the Entitlement Management Service.</p>
<p>zero to many groups</p> <pre><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ntk:AccessProfileValue></pre>	<p>2. One or more individuals are listed in the NTK Access Profile and the person's UIAS.XML^[37] digitalIdentifier attribute matches the "[IND_VALUE]" from the appropriate system identified by "individual:</p>
<p>zero to many individuals</p> <pre><ntk:AccessProfileValue ntk:vocabulary="individual:[IND_VOCAB]" >[IND_VALUE]</ntk:AccessProfileValue></pre>	<p>"individual: [IND_VOCAB]"</p>
	<p>a. When "[IND_VOCAB]" = "icpki" the entity has the UIAS.XML^[37] attribute certificateAuthority = "ICPKI" and digitalIdentifier = "[IND_VALUE]"</p> <p>b. When [IND_VOCAB] = "cadpki" the entity has the UIAS.XML^[37] attribute certificateAuthority = "CADPKI" and digitalIdentifier = "[IND_VALUE]"</p> <p>AND</p> <p>If NPE, MUST have UIAS.XML^[37] attribute</p>

ND-NTK	UIAS Attributes
	handlingControls containing "ND"

C.10.7 - Mapping ORCON to UIAS

This section discusses the relationship of OC markings on data objects to the entity attributes expressed in UIAS.XML^[37] with the focus on the agency dissemination **ntk:ProfileDes** for data markings. The ISM.XML^[27] **@ism:disseminationControls** value of "OC" requires an ORCON access policy be present. For resources marked with "OC-USGOV", distribution MAY be expanded beyond the implied distribution list through the use of Need-To-Know metadata. The basic access rules and mapping of UIAS.XML^[37] to OC-USGOV are found in ISM.ACES. If an OC-USGOV document includes Need-To-Know metadata that expands the list of authorized dissemination agencies beyond those automatically approved for OC-USGOV, then the access rules in this appendix apply.

The following Access Control Mapping table provides a mapping from specific ORCON Access Profile Need-To-Know elements to concrete UIAS.XML^[37] attributes. The "[ORIG_AGENCY]" and "[DISSEM_AGENCY]" tokens are placeholder values; these placeholders stand for actual agency acronyms used in an EXDIS Need-To-Know assertion. There may be multiple **ntk:AccessProfileValue** elements listing agencies authorized for dissemination.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.7 - Originator Controlled](#).



Note

- The ISM.ACES ORCON access rule does not apply in a SCOI and SCOI policies should be used instead. In a SCOI, the ORCON-NTK in a document should not be used for automated access decisions and instead use the list of authorized members of the SCOI.

Table 144 - ORCON Access Control Mapping

ntk:AccessProfile	UIAS Attributes
<p>ntk:AccessPolicy contains the ORCON URN</p> <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:oc </ntk:AccessPolicy></pre>	<p>The person or NPE MUST meet <i>at least one</i> of these criteria:</p> <ol style="list-style-type: none"> 1. The person or NPE UIAS.XML^[37] dutyOrganization matches "[ORIG_AGENCY]"
<p>ntk:ProfileDes contains the Agency Dissemination URN</p> <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:agencydissem </ntk:ProfileDes></pre>	
<p>exactly one originator agency</p> <pre><ntk:AccessProfileValue ntk:qualifier="originator" ntk:vocabulary="organization:usa- agency" >[ORIG_AGENCY]</ ntk:AccessProfileValue></pre>	<p>AND</p> <p>If NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "OC"</p>
<p>zero to many dissemtto agencies</p> <pre><ntk:AccessProfileValue ntk:qualifier="dissemtto" ntk:vocabulary="organization:usa- agency" >[DISSEM_AGENCY]</ ntk:AccessProfileValue></pre>	

C.10.8 - Mapping Permissive to UIAS

This section discusses the relationship of Restrictive constraints on data objects to the entity attributes expressed in the UIAS.XML^[37] specification.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.8 - Permissive](#).

Table 145 - Permissive Access Control Mapping

ntk:AccessProfile	UIAS Attribute
<p>ntk:AccessPolicy contains the Permissive URN</p> <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:permissive </ntk:AccessPolicy></pre>	<p>The user or NPE MUST meet <i>at least one</i> of these criteria:</p>
<p>ntk:ProfileDes contains the Group & Individual URN</p> <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre>	<p>1. One or more IAA Service Provider Entitlement Management Service groups are listed in the NTK Access Profile and the entity's UIAS.XML^[37] group attribute contains at least one "[GRP_VALUE]" from the Entitlement Management Service.</p>
<p>zero to many group vocabularies:</p> <pre><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ ntk:AccessProfileValue></pre>	<p>2. One or more individuals are listed in the NTK Access Profile and the person's UIAS.XML^[37] digitalIdentifier attribute matches the "[IND_VALUE]" from the appropriate system identified by "individual:[IND_VOCAB]"</p>
<p>and zero to many individual vocabularies:</p> <pre><ntk:AccessProfileValue ntk:vocabulary="individual:[IND_VOCAB]" >[IND_VALUE]</ntk:AccessProfileValue></pre>	<p>a. When "[IND_VOCAB]" = "icpki" the entity has the UIAS.XML^[37] attribute certificateAuthority = "ICPKI" and digitalIdentifier = "[IND_VALUE]"</p>
	<p>b. When "[IND_VOCAB]" = "cadpki" the entity has the UIAS.XML^[37] attribute certificateAuthority = "CADPKI" and digitalIdentifier = "[IND_VALUE]"</p>

C.10.9 - Mapping PROPIN to UIAS

C.10.9.1 - All US Government Employee PROPIN to UIAS Mapping

This section discusses the relationship of PROPIN markings on data objects to the entity attributes expressed in UIAS.XML^[37]. This section covers PROPIN access policy

"[urn:us:gov:ic:aces:ntk:propin:1](#)", which automatically permits dissemination to all employees of the United States Government. The ISM.XML^[27]

@[ism:disseminationControls](#) value of "PROPIN" requires a PROPIN access policy be present.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.9 - Proprietary Information for All US Government Employees](#).

For the purposes of this section, the expression "[USAgencyList]" refers to the list of organizations in the USAgency.CES^[38] Agency Acronym List with namespace [urn:us:gov:ic:cenum:usagency:agencyacronym](#).

Table 146 - All US Government Employee PROPIN Access List

ntk:AccessProfile	UIAS Attributes
<p>ntk:AccessPolicy contains the All USG PROPIN URN</p> <pre data-bbox="196 1094 927 1318" style="border: 1px solid blue; padding: 5px;"> <ntk:AccessProfile ism:classification="U" ism:ownerProducer="USA"> <ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:propin:1 </ntk:AccessPolicy> </ntk:AccessProfile></pre>	<p>The Person or NPE MUST meet <i>all</i> of the following:</p> <ol style="list-style-type: none"> 1. Have the entityType UIAS.XML^[37] attribute with a value of "MIL" or "GOV". 2. Have the adminOrganization UIAS.XML^[37] attribute exists in "[USAgencyList]". <p>AND</p> <p>If NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "PR"</p>

ntk:AccessProfile	UIAS Attributes
<p>ntk:AccessPolicy contains the All USG PROPIN URN</p> <pre data-bbox="196 342 928 436"><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:propin:1 </ntk:AccessPolicy></pre> <p>ntk:ProfileDes containing the Group & Individual URN</p> <pre data-bbox="196 569 928 663"><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre> <p>zero or more groups</p> <pre data-bbox="196 758 928 852"><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ntk:AccessProfileValue></pre> <p>zero or more individuals</p> <pre data-bbox="196 947 928 1041"><ntk:AccessProfileValue ntk:vocabulary="individual:[IND_VOCAB]" >[IND_VALUE]</ntk:AccessProfileValue></pre>	<p>The Person or NPE MUST meet <i>at least one</i> of the following:</p> <ol style="list-style-type: none"> 1. The Person or NPE meets <i>both</i> A and B: <ol style="list-style-type: none"> A. Have the entityType UIAS.XML^[37] attribute with a value of "MIL" or "GOV". B. Have the adminOrganization UIAS.XML^[37] attribute exists in "[USAgencyList]". 2. The person or NPE meets A or B: <ol style="list-style-type: none"> A. One or more IAA Service Provider Entitlement Management Service groups are listed in the Need-To-Know Access Profile and the entity's UIAS.XML^[37] group attribute contains at least one [GRP_VALUE] from the Entitlement Management Service. B. One or more individuals are listed in the Need-To-Know Access Profile and the person's UIAS.XML^[37] digitalIdentifier attribute matches the "[IND_VALUE]" from the appropriate system identified by "individual:[IND_VOCAB]" <ol style="list-style-type: none"> I. When "[IND_VOCAB]" = "icpki" the entity has the

ntk:AccessProfile	UIAS Attributes
	<p>UIAS.XML^[37] attribute certificateAuthority = "ICPKI" and digitalIdentifier = "[IND_VALUE]"</p> <p>II. When "[IND_VOCAB]" = "cadpki" the entity has the UIAS.XML^[37] attribute certificateAuthority = "CADPKI" and digitalIdentifier = "[IND_VALUE]"</p> <p>AND</p> <p>If NPE, MUST have UIAS.XML^[37] attribute handlingControls containing "PR"</p>

C.10.9.2 - PROPIN for Specified Members to UIAS Mapping

This section discusses the relationship of PROPIN markings on data objects to the entity attributes expressed in UIAS.XML^[37]. This section covers PROPIN access policy

"**urn:us:gov:ic:aces:ntk:propin:2**". This policy requires all authorized recipients to be explicitly listed in the PROPIN NTK access profile. That is, dissemination to employees of the US Government is NOT automatically authorized. The ISM.XML^[27]

@**ism:disseminationControls** value of "**PROPIN**" requires a PROPIN access policy be present.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.10 - Proprietary Information for Specified Members Only](#).

Table 147 - Group PROPIN Access List

ntk:AccessProfile	UIAS Attributes
ntk:AccessPolicy contains the Specified Members Only PROPIN URN	The person or NPE MUST meet <i>at least one</i> of the following:
<pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:propin:2 </ntk:AccessPolicy></pre>	1. One or more IAA Service Provider Entitlement Management Service groups are listed in the Need-To-Know Access Profile and the entity's UIAS.XML ^[37] group attribute contains at least one "[GRP_VALUE]" from the Entitlement Management Service.
ntk:ProfileDes containing the Group & Individual URN	
<pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre>	
zero or more groups	
<pre><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ntk:AccessProfileValue></pre>	2. One or more individuals are listed in the NTK Access Profile and the person's UIAS.XML ^[37] digitalIdentifier attribute matches the "[IND_VALUE]" from the appropriate system identified by "individual:[IND_VOCAB]"
zero or more individuals	
<pre><ntk:AccessProfileValue ntk:vocabulary="individual:[IND_VOCAB]" >[IND_VALUE]</ntk:AccessProfileValue></pre>	a. When "[IND_VOCAB]" = "icpki" the entity has the UIAS.XML ^[37] attribute certificateAuthority = "ICPKI" and digitalIdentifier = "[IND_VALUE]"
	b. When "[IND_VOCAB]" = "cadpki" the entity has the UIAS.XML ^[37] attribute certificateAuthority = "CADPKI" and digitalIdentifier = "[IND_VALUE]"
	AND

ntk:AccessProfile	UIAS Attributes
	If NPE, MUST have UIAS.XML ^[37] attribute handlingControls containing "PR"

C.10.10 - Mapping RAC to UIAS

This section discusses the relationship of RAC constraints on data objects to the entity attributes expressed in the UIAS.XML^[37] specification.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.12 - Restricted Authority Category](#).

Table 148 - RAC-NTK Access List

RAC-NTK	UIAS Attributes
ntk:AccessPolicy contains the RAC URN <pre><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:rac </ntk:AccessPolicy></pre>	The person or NPE MUST meet <i>all</i> of these criteria: <ol style="list-style-type: none"> 1. The value for the UIAS.XML^[37] authorityCategory attribute SHALL specify the PE's legal, policy, training, mission or other authorities to access and/or discover protected resources. 2. The PE record SHOULD contain all of its Authority Categories for which it is authorized. The value for the UIAS.XML^[37] authorityCategory attribute SHALL be updated by the managing program/agency/organization for the controlled vocabulary to manage, govern and expose the allowed values to the enterprise.
ntk:ProfileDes contains the Data Sphere URN <pre><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:datasphere </ntk:ProfileDes></pre>	
one to many RACs <pre><ntk:AccessProfileValue ntk:vocabulary="datasphere:rac" >[RAC]</ntk:AccessProfileValue></pre>	

C.10.11 - Mapping Restrictive to UIAS

This section discusses the relationship of Restrictive constraints on data objects to the entity attributes expressed in the UIAS.XML^[37] specification.

For the corresponding abstract person and NPE requirements that match the attributes in the table below, see [Section 5.9.13 - Restrictive](#).

Table 149 - Restrictive Access Control Mapping

ntk:AccessProfile	UIAS Attribute
<p>ntk:AccessPolicy contains the Restrictive URN</p> <pre data-bbox="196 369 928 466"><ntk:AccessPolicy> urn:us:gov:ic:aces:ntk:restrictive </ntk:AccessPolicy></pre>	<p>The Person or NPE MUST meet <i>all</i> of the following:</p>
<p>ntk:ProfileDes contains the Group & Individual URN</p> <pre data-bbox="196 562 928 659"><ntk:ProfileDes> urn:us:gov:ic:ntk:profile:grp-ind </ntk:ProfileDes></pre>	<ol style="list-style-type: none"> One or more IAA Service Provider Entitlement Management Service groups are listed in the Need-To-Know Access Profile and the entity's UIAS.XML^[37] group attribute contains ALL of the "[GRP_VALUE]" values.
<p>one or more groups</p> <pre data-bbox="196 751 928 848"><ntk:AccessProfileValue ntk:vocabulary="group:[GRP_VOCAB]" >[GRP_VALUE]</ntk:AccessProfileValue></pre>	<div data-bbox="943 716 1036 814"></div> <p>Warning</p> <p>If any @ntk:vocabulary attributes contain a "group:[GRP_VOCAB]" that is unknown to the system making the access control decision, then access must be denied.</p>

Appendix D Mapping ISM and UIAS Flow Control

D.1 - Introduction

This appendix discusses the relationship of ISM.XML^[27] attributes on data objects to the entity attributes expressed in UIAS.XML^[37] that relate specifically to flow control. Specifically, it gives an exact value-to-value mapping between the two specifications for Flow control purposes.

This section is currently only applicable to systems that know they are dealing with users who have non ICPKI certificates. A system that is receiving federated requests and believes those requests are always coming from a known network MAY ignore these restrictions. A system that has a user directly connecting SHOULD have both of these values available and SHOULD be making decisions based on them for that interaction.






Warning

Ignoring these restrictions is a risk posture decision for each system to make. Without these restrictions if the system receives federated queries they may be putting themselves at risk of spilling NF or partner restricted data.

D.2 - Certificate Authority

The matching abstract ISM.ACES attribute rules are contained in [Section 6.2 - Certificate Authority](#).

Table 150 - Certificate Authority



Person or NPE attributes sufficient for access	ISM Data Attributes
Unknown	<p>@ism:disseminationControls MUST contain "REL", @ism:releasableTo="[LIST]" list MUST contain all of "AUS", "CAN", "GBR", "NZL", "USA".</p> <div data-bbox="816 552 909 642"></div> <p>Note</p> <p>Some Tetragraphs such as "ACGU" are decomposable and therefore the combination of "ACGU" and "NZL" would satisfy this requirement.</p> <div data-bbox="816 793 909 884"></div> <p>Warning</p> <p>As Certificate Authority is optional a system MAY not have access to it. Lacking such information a system MUST not grant access to NF data.</p> <p>@ism:disseminationControls containing "NF" MUST not be allowed.</p> <p>@ism:nonICmarkings containing any of "SBU-NF", "LES-NF", "XD", "ND" MUST not be allowed.</p>
The certificate Authority is ICPKI	The use of an ICPKI certificate does not impact any flow control decisions.
The certificate Authority is CADPKI	<p>@ism:disseminationControls MUST contain "REL", @ism:releasableTo="[LIST]" list MUST contain more than "USA".</p> <div data-bbox="816 1545 909 1635"></div> <p>Warning</p> <p>@ism:disseminationControls containing "NF" MUST not be allowed.</p> <p>@ism:nonICmarkings containing any of "SBU-NF", "LES-NF", "XD", "ND" MUST not be allowed.</p>

D.3 - Originating Network

For the ISM.ACES abstract person and NPE requirements that match the attributes in the table below, see [Section 6.3 - Originating Network](#).

For the purposes of this section, the expression "[LIST]" refers to the list of countries within the RelTo CVE with namespace urn:us:gov:ic:cvenum:ismcat:relto. For a breakdown of tetragraph values in "[LIST]", please refer to *IC Markings System Register and Manual Annexes for Tetragraphs: IC Markings System Register and Manual Annex A* ^[11] or *IC Markings System Register and Manual Annex B* ^[12].

Table 151 - Originating Network

Person or NPE attributes sufficient for access	ISM Data Attributes
Unknown	<p>@ism:disseminationControls MUST contain "REL", @ism:releasableTo="[LIST]" list MUST contain all of "AUS", "CAN", "GBR", "NZL", "USA".</p> <div>  <p>Note</p> <p>Some Tetragraphs such as "ACGU" are decomposable and therefore the combination of "ACGU" and "NZL" would satisfy this requirement.</p> </div> <div>  <p>Warning</p> <p>As Originating Network is optional a system MAY not have access to it. Lacking such information a system MUST not grant access to NF data, or data not releasable to all of the FVEY countries.</p> <p>@ism:disseminationControls containing "NF" MUST not be allowed.</p> <p>@ism:nonICmarkings containing any of "SBU-NF", "LES-NF", "XD", "ND" MUST not be allowed.</p> </div>

Person or NPE attributes sufficient for access	ISM Data Attributes
The Originating Network is IMIS	<p>@ism:disseminationControls MUST contain "REL", @ism:releasableTo="[LIST]" list MUST contain all of "AUS", "GBR", "USA".</p> <div data-bbox="816 451 912 548"></div> <p>Warning</p> <p>@ism:disseminationControls containing "NF" MUST not be allowed.</p> <p>@ism:nonICmarkings containing any of "SBU-NF", "LES-NF", "XD", "ND" MUST not be allowed.</p>
The Originating Network is QNET	<p>@ism:disseminationControls MUST contain "REL", @ism:releasableTo="[LIST]" list MUST contain all of "AUS", "CAN", "GBR", "NZL", "USA".</p> <div data-bbox="816 989 912 1085"></div> <p>Note</p> <p>Some Tetragraphs such as "ACGU" are decomposable and therefore the combination of "ACGU" and "NZL" would satisfy this requirement.</p> <div data-bbox="816 1232 912 1329"></div> <p>Warning</p> <p>@ism:disseminationControls containing "NF" MUST not be allowed.</p> <p>@ism:nonICmarkings containing any of "SBU-NF", "LES-NF", "XD", "ND" MUST not be allowed.</p>
The Originating Network is NSANET	An Originating Network of NSANET does not impact any flow control decisions.
The Originating Network is JWICS	An Originating Network of JWICS does not impact any flow control decisions.

Appendix E Glossary

This appendix lists terms, definitions and sources of the definitions for terms used in this document.

attribute	<p>A distinct characteristic of an object. In the context of ICAM standards for PE and NPE entities, an attribute captures characteristics of PEs and NPEs.</p> <p>Source: ICS 500-30, <i>Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources</i> [25].</p>
Distinguished Name (DN)	<p>A unique name or character string that unambiguously identifies an entity according to the hierarchical naming conventions of X.500 directory service.</p> <p>Source: CNSS Instruction 4009, <i>National Information Assurance (IA) Glossary</i> [2].</p>
Entity	<p>An individual (person), organization, device, or process.</p> <p>Source: NIST 800-56Br1, <i>Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1</i> [35].</p>
Non-Person Entity (NPE)	<p>Entity related to Information Technology (IT), e.g., hardware objects (physical entities/devices) and software objects (virtual/logical entities).</p> <p>Source: ICS 500-30, <i>Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources</i> [25].</p>
Person Entity (PE)	<p>A human Entity that is the Owner of a PKI certificate (NIST SP 800-56Br1). A human entity that is the Name or Role Subscriber in a PKI certificate (CNSSI 1300).</p> <p>Source: NIST SP 800-56Br1, <i>Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 1</i> [35].</p> <p>Source: CNSSI 1300, <i>Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy under CNSS Policy No. 25</i> [1]</p>
token	<p>A token datatype is an XML schema language built-in datatype. A token datatype is a string datatype that contains one or more strings separated by a single space, e.g., <code>ism:releasableTo='USA AFG FVEY'</code> is an example of an ISM attribute that has token datatype. A token datatype contains no leading or trailing spaces, no carriage</p>

returns, no line feeds and no tab characters. The individual strings in an element or attribute that is a token datatype are referred to as tokens. In the `ism:releasableTo='USA AFG FVEY'` example, the tokens are 'USA', 'AFG' and 'FVEY'. In contrast, the value of `ism:releasableTo` is the entire string 'USA AFG FVEY'.

Source: <https://www.w3.org/TR/2004/REC-xmlschema-2-20041028/#token>

Appendix F List of Abbreviations

This appendix lists all the acronyms and abbreviations referenced in this encoding specification.

AC-3	NIST 800-53r4:ACCESS ENFORCEMENT
AC-4	NIST 800-53r4:INFORMATION FLOW ENFORCEMENT
ACES	Access Control Encoding Specification
AEA	Atomic Energy Act
ARH	Access Rights and Handling
CES	Controlled Vocabulary Enumeration Encoding Specification
CUI	Controlled Unclassified Information
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
E.O.	Executive Order
EXDIS	Exclusive Distribution
FD&R	Foreign Disclosure & Release
FOUO	For Official Use Only
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC ESB	Intelligence Community Enterprise Standards Baseline
ICO	Intelligence Community Only
ICPG	Intelligence Community Program Guidance
ICPM	Intelligence Community Policy Memorandum
ICS	Intelligence Community Standard

ISM	Information Security Markings
ISM.ACES	Access Control Encoding Specification for Information Security Marking
ISOO	Information Security Oversight Office
ISSM	Information Systems Security Manager
MN	Mission Need Profile
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
No Distribution	Data Encoding Specification for No Distribution Need-To-Know
NODIS	No Distribution
NPE	Non-Person Entity
NTK	Need-To-Know Metadata
OC	Originator Controlled
OC-NTK	Originator Controlled Need-to-Know
OC-USGOV	An Originator Control marking with implied distribution to a pre-determined list of United States Government agencies.
ORCON	Originator Controlled
PDP	Policy Decision Point
PE	Person Entity
PROPIN	Proprietary Information
SAP	Special Access Program
SAPCO	Special Access Program Control Office
SCI	Sensitive Compartmented Information
SCOI	Secure Community of Interest
TIC NG	Technical Integration Committee Next Generation
UIAS	Unified Identity Attribute Set
URI	Uniform Resource Identifier

URN	Uniform Resource Name
US	United States
USGOV	A designator that refers to a list of United States Government agencies pre-approved for distribution of specially marked Originator Controlled information.
XML	Extensible Markup Language

Appendix G Bibliography

[1] CNSSI 1300

Committee on National Security Systems. *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy under CNSS Policy No. 25*. 1300. December 2014.

Available online at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

[2] CNSSI 4009

Committee on National Security Systems. *National Information Assurance (IA) Glossary*. 4009. 6 April 2015.

Available online at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

[3] DoD Manual 5205.07

Under Secretary of Defense for Intelligence. *Special Access Program (SAP) Security Manual: Marking (Vol 4)*. 5205.07. October 10, 2013.

Available online at: <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520507-V4p.pdf?ver=2020-09-09-110203-730>

[4] E.O. 13526

The White House. *Executive Order 13526 – Classified National Security Information*. 29 December 2009.

Available online at: <http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>

[5] E.O. 13549

The White House. *Executive Order 13549 – Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*. August 18, 2010.

Available online at: <http://www.gpo.gov/fdsys/pkg/FR-2010-08-23/pdf/2010-21016.pdf>

[6] E.O. 13556

The White House. *Executive Order 13556 – Controlled Unclassified Information*. 4 November 2010.

Available online at: <https://www.archives.gov/files/isoo/policy-documents/eo-13556.pdf>

[7] FAC.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for Fine Access Control (FAC.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/uZz5l7T> (case sensitive – uniform Zulu zulu 5 India 7 Tango)

Available online Intelink-U at: <https://w3id.org/ic/standards/FAC>

Available online at: <https://w3id.org/ic/standards/public>

[8] IC CIO Memo 2018-081

Intelligence Community Chief Information Officer. *IC CIO Memo 2018-081: Improving Intelligence Community (IC) Identity, Credential, and Access Management (ICAM) to Achieve Greater Mission Effectiveness*. 26 November 2018.

[9] IC Markings

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*.

Available online Intelink-TS at: <https://go.ic.gov/tGXkwGO> (case sensitive – tango Golf Xray kilo whiskey Golf Oscar)

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>

[10] IC Markings DEC 2014

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register and Manual*. 31 Dec 2014.

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/icmarkings>

[11] IC Markings Annex A

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register Annex A, Tetragraph Table*.

Available online Intelink-TS at: <https://go.ic.gov/2VJrEQI> (case sensitive – 2 Victor Juliet romeo Echo Quebec India)

[12] IC Markings Annex B

Director of National Intelligence (DNI), Special Security Directorate (SSD), Security Markings Program (SMP). *Intelligence Community Markings System Register Annex B Authorized IC Tetragraphs*.

Available online Intelink-TS at: <https://go.ic.gov/ZqJuPEn> (case sensitive – Zulu quebec Juliet uniform Papa Echo november)

[13] IC-SF.XML

Office of the Director of National Intelligence. *Intelligence Community Specification Framework (IC-SF.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/pNFyuVg> (case sensitive – papa November Foxtrot yankee uniform Victor golf)

Available online Intelink-U at: <https://w3id.org/ic/standards/IC-SF>

Available online at: <https://w3id.org/ic/standards/public>

[14] ICD 208

Office of the Director of National Intelligence. *Write For Maximum Utility*. Intelligence Community Directive 208. 17 December 2008.

Available online at: http://www.dni.gov/files/documents/ICD/icd_208.pdf

[15] ICD 209

Office of the Director of National Intelligence. *Tearline Production and Dissemination*. Intelligence Community Directive 209. 6 September 2012.

Available online at: <http://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf>

[16] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online Intelink-TS at: <https://go.ic.gov/U7v6ZRL> (case sensitive – Uniform 7 victor 6 Zulu Romeo Lima)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[17] ICD 501

Office of the Director of National Intelligence. *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*. Intelligence Community Directive 501. 21 January 2009.

Available online Intelink-TS at: <https://go.ic.gov/FTBM8OS> (case sensitive – foxtrot Tango Bravo Mike 8 Oscar Sierra)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_501.pdf

[18] ICD 710

Office of the Director of National Intelligence. *Classification Management and Control Markings System*. Intelligence Community Directive 710. 21 June 2013.

Available online Intelink-TS at: <https://go.ic.gov/oSj9K7O> (case sensitive – oscar Sierra juliet 9 Kilo 7 Oscar)

Available online at: http://www.dni.gov/files/documents/ICD/ICD_710.pdf

[19] ICPG 500.2

Assistant Director of National Intelligence for Policy and Strategy. *Attribute-Based Authorization and Access Management*. Intelligence Community Policy Guidance 500.2. 23 November 2010.

Available online Intelink-TS at: <https://go.ic.gov/NUAEWk1> (case sensitive – November Uniform Alpha Echo Whiskey kilo 1)

Available online at: http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf

[20] ICPG 710.1

Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.

Available online Intelink-TS at: <https://go.ic.gov/fdyoylS> (case sensitive – foxtrot delta yankee oscar yankee India Sierra)

Available online at: <http://www.dni.gov/files/documents/ICPG/ICPG710.1.pdf>

[21] ICPG 710.2

Director of National Intelligence. *Application of Dissemination Controls: Foreign Disclosure and Release Markings*. Intelligence Community Policy Guidance 710.2. 20 March 2014.

Available online at: http://www.dni.gov/files/documents/ICPG/ICPG710-2_403-5.pdf

[22] ICPM 2007-200-2

Office of the Director of National Intelligence. *Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide*. Intelligence Community Policy Memorandum 2007-200-2. 11 December 2007.

Available online at: <http://www.dni.gov/files/documents/IC%20Policy%20Memos/ICPM%202007-200-2%20Responsibility%20to%20Provide.pdf>

[23] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.

Available online Intelink-TS at: <https://go.ic.gov/kh8NMVJ> (case sensitive – kilo hotel 8 November Mike Victor Juliet)

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-20>

[24] ICS 500-21

Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.

Available online Intelink-TS at: <https://go.ic.gov/0Agmenr> (case sensitive – 0 Alpha golf mike echo november romeo)

Available online Intelink-U at: <https://w3id.org/ic/standards/policy/ICS500-21>

[25] ICS 500-30

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources*. Intelligence Community Standard 500-30. 24 April 2014.

Available online Intelink-TS at: <https://go.ic.gov/lqk775v> (case sensitive – lima quebec kilo 7 7 5 victor)

[26] ISM.ACES

Office of the Director of National Intelligence. *Access Control Encoding Specification for Information Security Markings (ISM.ACES)*.

Available online Intelink-TS at: <https://go.ic.gov/rOG2Bjt> (case sensitive – romeo Oscar Golf 2 Bravo juliet tango)

Available online Intelink-U at: <https://w3id.org/ic/standards/ISM-ACES>

Available online at: <https://w3id.org/ic/standards/public>

[27] ISM.XML

Office of the Director of National Intelligence. *XML Data Encoding Specification for Information Security Markings (ISM.XML)*.

Available online Intelink-TS at: <https://go.ic.gov/qoNICy7> (case sensitive – quebec oscar November India Charlie yankee 7)

Available online Intelink-U at: <https://w3id.org/ic/standards/ISM>

Available online at: <https://w3id.org/ic/standards/public>

[28] ISMCAT.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for ISM Country Codes and Tetragraphs (ISMCAT.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/mL5WA9> (case sensitive – mike Lima Foxtrot 5 Whiskey Alpha 9)

Available online Intelink-U at: <https://w3id.org/ic/standards/ISMCAT>

Available online at: <https://w3id.org/ic/standards/public>

[29] ISOO 32 CFR Parts 2001 and 2003

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Classified National Security Information; Final Rule*. 32 CFR Parts 2001 and 2003. Federal Register, Vol. 75, No. 123. 28 June 2010.

Available online at: <http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf>

[30] ISOO 32 CFR Part 2002

Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *Controlled Unclassified; Final Rule*. 32 CFR Parts 2002. Federal Register, Vol. 81, No. 178. 14 September 2016.

- Available online at: <https://www.archives.gov/files/isoo/policy-documents/32-cfr-part-2002.pdf>
- [31] ISOO 32 CFR Parts 2003
Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *The Interagency Security Classification Appeals Panel (ISCAP) Bylaws, Rules, and Appeal Procedures*. 32 CFR Parts 2003. Federal Register, Vol. 77, No. 131. 9 July 2012.
Available online at: <https://www.archives.gov/files/isoo/policy-documents/32-cfr-part-2003.pdf>
- [32] ISOO 32 CFR Parts 2004 Amendment
Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). *National Industrial Security Program Directive No. 1*. 32 CFR Parts 2004. Federal Register, Vol. 75, No. 65. 6 April 2010.
Available online at: <https://www.archives.gov/files/isoo/policy-documents/32-cfr-part-2004-amendment.pdf>
- [33] ISOO Marking Booklet 2018
Information Security Oversight Office. *Marking Classified National Security Information 2018*. Rev. 4, January 2018.
Available online at: <https://www.archives.gov/files/isoo/training/marketing-booklet-revision.pdf>
- [34] NIST 800-53r4
National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*. Revision 4. April 2013.
Available online at: <http://dx.doi.org/10.6028/NIST.SP.800-53r4>
- [35] NIST 800-56Br1
National Institute of Standards and Technology. *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. Revision 1. September 2014.
Available online at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf>
- [36] PE-Portal
ODNI/Partner Engagement Tetragraph Portal. Office of the Director of National Intelligence
Available online Intelink-TS at: <https://intellipedia.intelink.ic.gov/wiki/Portal:Tetragraphs>
Available online Intelink-S at: <https://intellipedia.intelink.sgov.gov/wiki/Portal:Tetragraphs>
- [37] UIAS.XML
Office of the Director of National Intelligence. *IC Enterprise Attribute Exchange Between IC Attribute Services Unified Identity Attribute Set (UIAS.XML)*.
Available online Intelink-TS at: <https://go.ic.gov/xQK4AX1> (case sensitive – xray Quebec Kilo 4 Alpha Xray 1)
Available online Intelink-U at: <https://w3id.org/ic/standards/UIAS>
Available online at: <https://w3id.org/ic/standards/public>
- [38] USAgency.CES

Office of the Director of National Intelligence. *CVE Encoding Specification for US Agency Acronyms (USAgency.CES)*.

Available online Intelink-TS at: <https://go.ic.gov/wmyIRCV> (case sensitive – whiskey mike yankee India Romeo Charlie Victor)

Available online Intelink-U at: <https://w3id.org/ic/standards/USAgency>

Available online at: <https://w3id.org/ic/standards/public>

Appendix H Points of Contact

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at the following DNI-sponsored web sites.

Public Website: <https://w3id.org/ic/standards/public>

Intelshare: <https://w3id.org/ic/standards/data-specs>

Direct all inquiries about this IC technical specification, IC technical specification collaboration and coordination forums, or IC element representatives involved in those forums, to the IC CIO.

E-mail: ic-standards-support@odni.gov.

Appendix I IC CIO Approval Memo

An IC CIO Approval Memo should accompany this enterprise technical data specification bearing the signature of the IC CIO or an IC CIO-designated official(s). If an IC CIO Approval Memo is not accompanying this specification's version release package, then refer back to the authoritative web location(s) for this specification to see if a more complete package or a specification update is available.

Specification artifacts display a date representing the last time a version's artifacts as a whole were modified. This date most often represents the conclusion of the IC Element collaboration and coordination process. Once the IC Element coordination process is complete, the specification goes through an internal IC CIO staffing and coordination process leading to signature of the IC CIO Approval Memo. The signature date of the IC CIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the IC CIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC ESB as defined in ICS 500-20^[23].