



# **Controlled Vocabulary Enumeration Values for ISM**

---

## **ISM-CVEnums**

**Version 2021-NOVr2022-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 - CVEnumISM25X for ISM .....	1
1.1 - Descriptive information .....	1
1.2 - Permissible Values .....	1
Chapter 2 - CVEnumISMatomicEnergyMarkings for ISM .....	4
2.1 - Descriptive information .....	4
2.2 - Permissible Values .....	4
Chapter 3 - CVEnumISMAttributes for ISM .....	5
3.1 - Descriptive information .....	5
3.2 - Permissible Values .....	5
Chapter 4 - CVEnumISMClassificationAll for ISM .....	7
4.1 - Descriptive information .....	7
4.2 - Permissible Values .....	7
Chapter 5 - CVEnumISMClassificationUS for ISM .....	8
5.1 - Descriptive information .....	8
5.2 - Permissible Values .....	8
Chapter 6 - CVEnumISMCompliesWith for ISM .....	9
6.1 - Descriptive information .....	9
6.2 - Permissible Values .....	9
Chapter 7 - CVEnumISMCUIBasic for ISM .....	11
7.1 - Descriptive information .....	11
7.2 - Permissible Values .....	11
Chapter 8 - CVEnumISMCUISpecified for ISM .....	23
8.1 - Descriptive information .....	23
8.2 - Permissible Values .....	23
Chapter 9 - CVEnumISMDissem for ISM .....	32
9.1 - Descriptive information .....	32
9.2 - Permissible Values .....	32
Chapter 10 - CVEnumISMDissemCommingled for ISM .....	34
10.1 - Descriptive information .....	34
10.2 - Permissible Values .....	34
Chapter 11 - CVEnumISMDissemCui for ISM .....	36
11.1 - Descriptive information .....	36
11.2 - Permissible Values .....	36
Chapter 12 - CVEnumISMDissemIcrm for ISM .....	37
12.1 - Descriptive information .....	37
12.2 - Permissible Values .....	37
Chapter 13 - CVEnumISMElements for ISM .....	38
13.1 - Descriptive information .....	38
13.2 - Permissible Values .....	38
Chapter 14 - CVEnumISMExemptFrom for ISM .....	39
14.1 - Descriptive information .....	39
14.2 - Permissible Values .....	39
Chapter 15 - CVEnumISMHighWaterNATO for ISM .....	40
15.1 - Descriptive information .....	40
15.2 - Permissible Values .....	40
Chapter 16 - CVEnumISMNonIC for ISM .....	41

16.1 - Descriptive information .....	41
16.2 - Permissible Values .....	41
Chapter 17 - CVEnumISMNonUSControls for ISM .....	42
17.1 - Descriptive information .....	42
17.2 - Permissible Values .....	42
Chapter 18 - CVEnumISMNotice for ISM .....	43
18.1 - Descriptive information .....	43
18.2 - Permissible Values .....	43
Chapter 19 - CVEnumISMNoticeProse for ISM .....	45
19.1 - Descriptive information .....	45
19.2 - Permissible Values .....	45
Chapter 20 - CVEnumISMPocType for ISM .....	49
20.1 - Descriptive information .....	49
20.2 - Permissible Values .....	49
Chapter 21 - CVEnumISMSAR for ISM .....	50
21.1 - Descriptive information .....	50
21.2 - Permissible Values .....	50
Chapter 22 - CVEnumISMSARAuthorities for ISM .....	51
22.1 - Descriptive information .....	51
22.2 - Permissible Values .....	51
Chapter 23 - CVEnumISMSCIControls for ISM .....	52
23.1 - Descriptive information .....	52
23.2 - Permissible Values .....	52
Chapter 24 - CVEnumISMSecondBannerLine for ISM .....	54
24.1 - Descriptive information .....	54
24.2 - Permissible Values .....	54
Chapter 25 - CVEnumNTKAccessPolicy for ISM .....	55
25.1 - Descriptive information .....	55
25.2 - Permissible Values .....	55
Chapter 26 - CVEnumNTKProfileDes for ISM .....	57
26.1 - Descriptive information .....	57
26.2 - Permissible Values .....	57

## List of Tables

Table 1 - CVEnumISM25X Values .....	1
Table 2 - CVEnumISMatomicEnergyMarkings Values .....	4
Table 3 - CVEnumISMAttributes Values .....	5
Table 4 - CVEnumISMClassificationAll Values .....	7
Table 5 - CVEnumISMClassificationUS Values .....	8
Table 6 - CVEnumISMCompliesWith Values .....	9
Table 7 - CVEnumISMCUIBasic Values .....	11
Table 8 - CVEnumISMCUISpecified Values .....	23
Table 9 - CVEnumISMDissem Values .....	32
Table 10 - CVEnumISMDissemCommingled Values .....	34
Table 11 - CVEnumISMDissemCui Values .....	36
Table 12 - CVEnumISMDissemIcrm Values .....	37
Table 13 - CVEnumISMElements Values .....	38
Table 14 - CVEnumISMExemptFrom Values .....	39
Table 15 - CVEnumISMHighWaterNATO Values .....	40
Table 16 - CVEnumISMNonIC Values .....	41
Table 17 - CVEnumISMNonUSControls Values .....	42
Table 18 - CVEnumISMNotice Values .....	43
Table 19 - CVEnumISMNoticeProse Values .....	45
Table 20 - CVEnumISMPocType Values .....	49
Table 21 - CVEnumISMSAR Values .....	50
Table 22 - CVEnumISMSARAuthorities Values .....	51
Table 23 - CVEnumISMSCIControls Values .....	52
Table 24 - CVEnumISMSecondBannerLine Values .....	54
Table 25 - CVEnumNTKAccessPolicy Patterns .....	55
Table 26 - CVEnumNTKAccessPolicy Values .....	55
Table 27 - CVEnumNTKProfileDes Values .....	57

## Chapter 1 - CVEnumISM25X for ISM

### 1.1 - Descriptive information

- Description: All currently authorized authority block declass date/event exemptions. This CVE is used by @ism:declassException.
- Multiplicity: Multi-Valued Max Values: 25
- URN: urn:us:gov:ic:cvenum:ism:25x
- Created: 2012-01-04T02:15:00-04:00
- Source: Marking Classified National Security Information Directive No. 1
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 1.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISM25X.xml

**Table 1 - CVEnumISM25X Values**

CVEnumISM25X Values	
Value	Documentation
AEA	When using a source document that contains portions of Restricted Data (RD) or Formerly Restricted Data (FRD) where the RD/FRD source document(s) do not have declassification instructions, the derivatively classified document shall not contain a declassification date or event on the Declassify On line. The following shall be annotated on the Declassify On line: "Not Applicable or (N/A) to RD/FRD portions" and "See source list for NSI portions" separated by a period. The source list must include the declassification instruction for each of the source documents classified under E.O. 13526 and shall not appear in the classification authority block
NATO	Since NATO information is not to be declassified or downgraded without the prior consent of NATO, the "Declassify on" line of documents that commingle information classified by NATO and U.S. classified NSI, will read "N/A to NATO portions. See source list for NSI portions." The NSI source list will appear beneath the classification authority block in a manner that clearly identifies it as separate and distinct.
NATO-AEA	Handles special case of BOTH NATO and AEA as a single exemption.

CVEnumISM25X Values	
Value	Documentation
25X1	Reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.
25X1-EO-12951	"25X1, EO 12951" (prescribed by the DNI for use on information described in E.O. 12951, Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems)
25X2	Reveal information that would assist in the development, production, or use of weapons of mass destruction.
25X3	Reveal information that would impair U.S. cryptologic systems or activities.
25X4	Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system.
25X5	Reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;
25X6	Reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States
25X7	Reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized.
25X8	Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security.
25X9	Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.
50X1	The ISCAP has authorized use of this code in the FBI's classification guidance (which results in a 75-year classification period) for any agency sourcing/reusing the information.
50X1-HUM	When the information clearly and demonstrably could be expected to reveal the identity of a confidential human source or a human intelligence source.
50X2	Reveal information that would assist in the development, production, or use of weapons of mass destruction.

<b>CVEnumISM25X Values</b>	
<b>Value</b>	<b>Documentation</b>
50X2-WMD	When the information clearly and demonstrably could reveal key design concepts of weapons of mass destruction.
50X3	Reveal information that would impair U.S. cryptologic systems or activities.
50X4	Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system.
50X5	Reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;
50X6	Reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States
50X7	Reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized.
50X8	Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security.
50X9	Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.
75X	Specific information that has been formally approved by the ISCAP as information that does not permit the automatic or unilateral declassification of information at 75 years.

## Chapter 2 - CVEnumISMatomicEnergyMarkings for ISM

### 2.1 - Descriptive information

- Description: All currently valid Atomic Energy information markings from the published register. This CVE is used by @ism:atomicEnergyMarkings.
- Multiplicity: Multi-Valued Max Values: 14
- URN: urn:us:gov:ic:cvenum:ism:atomicEnergyMarkings
- Created: 2011-02-04T00:22:00-04:00
- Source: IC Systems Register and Manual
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 2.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMatomicEnergyMarkings.xml

**Table 2 - CVEnumISMatomicEnergyMarkings Values**

CVEnumISMatomicEnergyMarkings Values	
Value	Documentation
RD	RESTRICTED DATA
RD-CNWDI	RD-CRITICAL NUCLEAR WEAPON DESIGN INFORMATION
RD-SG-14	RD-SIGMA-14
RD-SG-15	RD-SIGMA-15
RD-SG-18	RD-SIGMA-18
RD-SG-20	RD-SIGMA-20
FRD	FORMERLY RESTRICTED DATA
FRD-SG-14	RD-SIGMA-14
FRD-SG-15	RD-SIGMA-15
FRD-SG-18	RD-SIGMA-18
FRD-SG-20	RD-SIGMA-20
DCNI	DoD CONTROLLED NUCLEAR INFORMATION
UCNI	DoE CONTROLLED NUCLEAR INFORMATION
TFNI	TRANSClassified FOREIGN NUCLEAR INFORMATION

## Chapter 3 - CVEnumISMAttributes for ISM

### 3.1 - Descriptive information

- Description: All currently authorized ISM attribute names. This file is not imported by the schema.
- Multiplicity: Multi-Valued Max Values: 47
- URN: urn:us:gov:ic:cvenum:ism:attributes
- Created: 2010-05-30T16:52:00-04:00
- Source: ISM schema
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 3.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMAttributes.xml

**Table 3 - CVEnumISMAttributes Values**

CVEnumISMAttributes Values	
Value	Documentation
compliesWith	compliesWith attribute
classification	classification attribute
ownerProducer	ownerProducer attribute
SCIcontrols	SCIcontrols attribute
SARIdentifier	SARIdentifier attribute
atomicEnergyMarkings	atomicEnergyMarkings attribute
disseminationControls	disseminationControls attribute
FGIsourceOpen	FGIsourceOpen attribute
FGIsourceProtected	FGIsourceProtected attribute
hasApproximateMarkings	hasApproximateMarkings attribute
releasableTo	releasableTo attribute
displayOnlyTo	displayOnlyTo attribute
nonICmarkings	nonICmarkings attribute
classifiedBy	classifiedBy attribute
derivativelyClassifiedBy	derivativelyClassifiedBy attribute
classificationReason	classificationReason attribute
nonUSControls	nonUSControls attribute
derivedFrom	derivedFrom attribute

CVEnumISMAttributes Values	
Value	Documentation
declassDate	declassDate attribute
declassEvent	declassEvent attribute
declassException	declassException attribute
resourceElement	resourceElement attribute
highWaterNATO	highWaterNATO attribute
excludeFromRollup	excludeFromRollup attribute
createDate	createDate attribute
compilationReason	compilationReason attribute
noAggregation	noAggregation attribute
noticeType	noticeType attribute
noticeProseID	noticeProseID attribute
externalNotice	externalNotice attribute
DESVersion	DESVersion attribute
ISMCATCESVersion	ISMCATCESVersion attribute
noticeDate	notice date attribute
noticeReason	notice Reason attribute
exemptFrom	exemptFrom attribute
unregisteredNoticeType	unregisteredNoticeType attribute
pocType	Specifies a point-of contact for a security-related requirement.
joint	Indicator that multiple ownerProducers should be interpreted as JOINT.
cuiBasic	CUI Basic markings.
cuiSpecified	CUI Specified markings.
cuiDecontrolDate	Decontrol date for CUI.
cuiDecontrolEvent	Decontrol event for CUI.
cuiControlledBy	Person or authority for labeling and controlling information as CUI.
cuiControlledByOffice	Office in an agency or department that is responsible for labeling and controlling information as CUI. Ref DOD INSTRUCTION 5200.48.
cuiPOC	Point of Contact for labeling and controlling information as CUI. Ref DOD INSTRUCTION 5200.48.
secondBannerLine	Tokens that contain markings used to support administrative and legal processes for handling and protecting documents. When they appear in a document, these tokens form a second line that is placed below the banner.
handleViaChannels	Handle VIA Channels that may appear in the second banner line.

## Chapter 4 - CVEnumISMClassificationAll for ISM

### 4.1 - Descriptive information

- Description: All currently valid classification marks. This CVE is used by @ism:classification.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:ism:classification:all
- Created: 2010-05-31T21:22:00-04:00
- Source: IC Systems Register and Manual
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 4.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMClassificationAll.xml

**Table 4 - CVEnumISMClassificationAll Values**

CVEnumISMClassificationAll Values	
Value	Documentation
R	RESTRICTED
C	CONFIDENTIAL
S	SECRET
TS	TOP SECRET
U	UNCLASSIFIED

## Chapter 5 - CVEnumISMClassificationUS for ISM

### 5.1 - Descriptive information

- Description: All currently valid US classification marks. This file is not imported by the schema.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:ism:classification:us
- Created: 2010-03-12T11:29:00-04:00
- Source: IC Systems Register and Manual
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 5.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMClassificationUS.xml

**Table 5 - CVEnumISMClassificationUS Values**

CVEnumISMClassificationUS Values	
Value	Documentation
TS	TOP SECRET
S	SECRET
C	CONFIDENTIAL
U	UNCLASSIFIED

## Chapter 6 - CVEnumISMCompliesWith for ISM

### 6.1 - Descriptive information

- Description: ISM rule sets documents may comply with. This CVE is used by @ism:compliesWith.
- Multiplicity: Multi-Valued Max Values: 6
- URN: urn:us:gov:ic:cvenum:ism:complieswith
- Created: 2010-05-30T16:52:00-04:00
- Source: ISM schema
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 6.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMCompliesWith.xml

**Table 6 - CVEnumISMCompliesWith Values**

CVEnumISMCompliesWith Values	
Value	Documentation
USGov	Document claims compliance with all rules encoded in ISM for documents produced by the US Federal Government. This is the minimum set of rules for US documents to adhere to, and all US documents should claim compliance with USGov. For example, a US Intelligence Community document should claim ism:compliesWith="USGov USIC".
USIC	Document claims compliance with all rules encoded in ISM for documents produced by the US Intelligence Community. Documents that claim compliance with USIC MUST also claim compliance with USGov.
USDOD	Document claims compliance with all rules encoded in ISM for documents produced by the US Department of Defense. Documents that claim compliance with USDOD MUST also claim compliance with USGov.
OtherAuthority	Document claims compliance with an authority other than the USGov, USIC, or USDOD. This token is not allowed if the ism:ownerProducer contains USA.
USA-CUI-ONLY	Document is UNCLASSIFIED and was created in an UNCLASSIFIED environment. Document claims compliance with CUI rules but with no USGOV rules for classified environments. Special transforms are required to move the document into a classified environment or to commingle content from this document with any content created in a classified environment.

<b>CVEnumISMCompliesWith Values</b>	
<b>Value</b>	<b>Documentation</b>
USA-CUI	Document contains both NSI (National Security Information) and CUI according to DoD rules for CUI. Document claims compliance with 1. CUI rules according to DoD, and 2. USGOV and/or USDOD rules for classified environments.

## Chapter 7 - CVEnumISMCUIBasic for ISM

### 7.1 - Descriptive information

- Description: All currently valid CUI Basic markings from the National Archives. This CVE is used by @ism:cuiBasic.
- Multiplicity: Multi-Valued Max Values: 93
- URN: urn:us:gov:ic:cvenum:ism:cuibasic
- Created: 2019-08-16T16:14:00-05:00
- Source: National Archives CUI Category Markings
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 7.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMCUIBasic.xml

**Table 7 - CVEnumISMCUIBasic Values**

CVEnumISMCUIBasic Values	
Value	Documentation
ADPO	Administrative Proceedings. Adjudication of agency-related matters including, but not limited to, dispute resolution, settlements, and issuances of orders.
AG	Agriculture. Information related to the agricultural operation, farming or conservation practices, or the actual land of an agricultural producer or landowner.
ASYL	Asylee. Related to refugee applications and associated hearings to grant asylum to foreign nationals in the United States to be recognized as asylees.

CVEnumISMCUIBasic Values	
Value	Documentation
FSEC	Bank Secrecy. Information that is provided to the government pursuant to the Bank Secrecy Act, including but not limited to, suspicious activity reports (SAR), currency transaction reports (CTR), reports of international transportation of currency or monetary instruments (CMIR), reports of cash payment over \$10,000 received in trade or business, and reports of foreign bank and financial accounts (FBAR). Reports filed under the Bank Secrecy Act (BSA), codified in relevant part at 31 U.S.C. § 5311 et seq, are specifically exempt from disclosure under the Freedom of Information Act, codified at 5 U.S.C. § 552, and also may not be disclosed under any State, local, tribal, or territorial “freedom of information,” “open government,” or similar law. See 31 U.S.C. § 5319; 5 U.S.C. § 552(b) (3). These reports (BSA Reports), are maintained in a system of records containing information compiled for law enforcement investigative purposes that has been exempted from the access provisions of the Privacy Act in accordance with 5 U.S.C. §§ 552a(j) (2) and (k)(2). BSA Reports may only be re-disseminated in strict accordance with guidelines established by the Financial Crimes Enforcement Network (FinCEN), the Treasury bureau that administers the BSA. Suspicious Activity Reports, one of the types of required reports filed under the BSA, are required to be kept confidential in accordance with 31 U.S.C. § 5318(g)(2) and implementing regulations. To the extent information falling under the purview of the BSA is collected, accessed, or used for any Federal tax administration purpose, it is also subject to the confidentiality provisions of the Internal Revenue Code, codified at 26 U.S.C. § 6103.
BATT	Battered Spouse or Child. Related to information within applications and associated hearings provided by, or that could identify, a battered spouse or child of a US citizen or US permanent resident seeking independent protected status within the United States.
CVI	Chemical-terrorism Vulnerability Information. In accordance with Section 550(c) of the Department of Homeland Security Appropriations Act of 2007, the following information, whether transmitted verbally, electronically, or in written form, shall constitute CVI, see (1) - (9).
CVIC	Child Victim/Witness. Information pertaining to a minor who was a victim, witness, or potential witness to a criminal act.
BARG	Collective Bargaining. Defining agencies' and representatives' duty to negotiate in good faith to include disclosure of certain labor relations training and guidance materials and limiting the issuance of certain subpoenas.
CMPRS	Committed Person. Related to information concerning the mental condition of a person committed to a psychiatric facility.

<b>CVEnumISMCUIBasic Values</b>	
<b>Value</b>	<b>Documentation</b>
LCOMM	Communications. Related to the contents of any wire, oral, or electronic communication.
COMPT	Comptroller General. Concerning the Officer of the United States Government who is charged with duties relating to fiscal affairs, including auditing, examining accounts, and reporting the financial status of the United States Government.
DREC	Death Records. Related to information contained within an official document issued by a public registry verifying that a person has died, with information such as the date and time of death, the cause of death, and the signature of the attending or examining physician.
DCRIT	DoD Critical Infrastructure Security Information. Information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated on behalf of the DoD, including vulnerability assessments prepared by or on behalf of the DoD, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security.
XFER	Electronic Funds Transfer. Relating to the computer-based systems used to perform financial transactions electronically.
EMGT	Emergency Management. Related to information concerning the continuity of executive branch operations during all-hazards emergencies or other situations that may disrupt normal operations.
EXPT	Export Controlled. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.
EXPTR	Export Controlled Research. Related to the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions.

CVEnumISMCUIBasic Values	
Value	Documentation
JURY	Federal Grand Jury. Material obtained pursuant to a federal grand jury subpoena, which includes (1) any reference to a specific sitting grand jury; (2) any documentation or data obtained by a grand jury subpoena if disclosure of such material tends to reveal what transpired before or at the direction of the federal grand jury; (3) documentation prepared specifically for the federal grand jury; and (4) transcripts or other recordings of testimony presented to the federal grand jury.
FHFANPI	Federal Housing Finance Non-Public Information. Related to information that the Federal Housing Finance Agency (FHFA) has not made public that is created by, obtained by, or communicated to an FHFA employee in connection with the performance of official duties, regardless of who is in possession of the information, including confidential supervisory information. Confidential supervisory information includes FHFA reports of examination, inspection and visitation, confidential operating and condition reports, and any information derived from, related to, or contained in such reports, or gathered by FHFA in the course of any investigation, suspicious activity report, cease-and-desist order, civil money penalty enforcement order, suspension, removal or prohibition order, or other supervisory or enforcement orders or actions taken under the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, and other conditions as set forth in 12 CFR Part 1214.1.
FSI	Financial Supervision Information. Related to information connected to an agency's responsibilities to supervise, examine, and evaluate a financial institution.
CRIT	General Critical Infrastructure Information. Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.
FNC	General Financial Information. Related to the duties, transactions, or otherwise falling under the purview of financial institutions or United States Government fiscal functions. Uses may include, but are not limited to, customer information held by a financial institution.
INTEL	General Intelligence. Related to intelligence activities, sources, or methods.
LEI	General Law Enforcement. Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions.
NUC	General Nuclear. Related to protection of information concerning nuclear reactors, materials, or security.

<b>CVEnumISMCUIBasic Values</b>	
<b>Value</b>	<b>Documentation</b>
PRVCY	General Privacy. Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-17-12, or "means of identification" as defined in 18 USC 1028(d)(7).
PROPIN	General Proprietary Business Information. Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.
GENETIC	Genetic Information. The term "genetic information" means, with respect to any individual, information about-- (i) such individual's genetic tests, (ii) the genetic tests of family members of such individual, and (iii) the manifestation of a disease or disorder in family members of such individual.
HLTH	Health Information. As per 42 USC 1320d(4), "health information" means any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
CUI-PROVISIONAL-HSAI	Provisional - Homeland Security Agreement Information. Information DHS receives and is required to protect pursuant to an agreement with state, local, tribal, territorial, and private sector partners. DHS receives this information in furtherance of the missions of the Department, including but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Security Act.
CUI-PROVISIONAL-HSEI	Provisional - Homeland Security Enforcement Information. Unclassified information of a sensitive nature lawfully created, possessed, or transmitted by DHS in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department.
INF	Informant. Related to the identity of a human source.
ISVI	Information Systems Vulnerability Information. Related to information that if not protected, could result in adverse effects to information systems. Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

CVEnumISMCUIBasic Values	
Value	Documentation
CUI-PROVISIONAL-ISVIH	Provisional - Information Systems Vulnerability Information - Homeland. a. DHS information technology internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526, will be classified as appropriate. b. Information regarding developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to close, counterfeit, or circumvent a process or system.
PRIIG	Inspector General Protected. Related to the identity of a person making a report to the Inspector General of any Executive agency.
ID	Internal Data. Refers to a category of information that is not intended to be disseminated beyond CIA channels that involves intelligence activities, sources, or methods. This information may also relate to the CIA's organization, functions, names, official titles, salaries, or numbers of personnel.
CUI-PROVISIONAL-IAIH	Provisional - International Agreement Information - Homeland. Information DHS receives and is required to protect pursuant to an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization.
FINT	International Financial Institutions. Relating to entities that provide financial services for its clients or members, and were established (or chartered) by more than one country, and hence are subjects of international law.
INVENT	Inventions. An invention is any art or process (way of doing or making things), machine, manufacture, design, or composition of matter, or any new and useful improvement thereof, or any variety of plant, which is or may be patentable under the patent laws of the United States, in which the federal government owns or may own a right, title, or interest.
INV	Investigation. Related to information obtained during the course of a law enforcement investigation or action, civil or criminal.
SURV	Investment Survey. Information reported to Treasury, the Federal Reserve Board of Governors, or the Federal Reserve Banks as part of the Treasury International Capital (TIC) data reporting system.
JUV	Juvenile. Related to the identity of individual juvenile youths.

CVEnumISMCUIBasic Values	
Value	Documentation
PRIVILEGE	Legal Privilege. Per 12 USC 78x: The term "privilege" includes any work-product privilege, attorney-client privilege, governmental privilege, or other privilege recognized under Federal, State, or foreign law. Per 502(g): (1) "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and (2) "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.
LMI	Legislative Materials. Data related to Congress's legislative, investigatory or oversight responsibilities of the Executive branch of the Federal government. This includes data related to proposed or pending legislation as well as inquiries submitted by Congress to Federal agencies, agency responses to those inquiries and any other information which, if disclosed, would reveal the nature and scope of Congressional inquiries.
MERG	Mergers. Relating to methods by which corporations legally unify ownership of assets formerly subject to separate controls.
MIL	Military Personnel Records. Any member or former member of the armed forces or affiliated organization of the Department of Defense.
LNSL	National Security Letter. Related to administrative orders sent to compel the recipients of the letters to provide information to federal investigators.
NETW	Net Worth. Related to the net worth of an individual and/or their affiliates in certain administrative proceedings.
NNPI	Naval Nuclear Propulsion Information. Related to the safety of reactors and associated naval nuclear propulsion plants, and control of radiation and radioactivity associated with naval nuclear propulsion activities, including prescribing and enforcing standards and regulations for these areas as they affect the environment and the safety and health of workers, operators, and the general public.
OPSEC	Critical information determined to give evidence of the planning and execution of sensitive (frequently classified) government activities after going through a formal systematic vetting process in accordance with National Security Decision Directive Number 298. This process identifies unclassified information that must be protected. It almost always results from an agency's official OPSEC program, or is otherwise commonly approved for use by the CUI Senior Agency Official.
RECCOM	Nuclear Recommendation Material. Related to recommendations to the Secretary of Energy with respect to Department of Energy defense nuclear facilities as determined necessary to ensure adequate protection of public health and safety.

<b>CVEnumISMCIUBasic Values</b>	
<b>Value</b>	<b>Documentation</b>
SRI	Nuclear Security-Related Information. Related to information that could be useful, or could reasonably be expected to be useful, to a terrorist in a potential attack that does not qualify as Safeguards or classified information, including the exact location and quantities of radioactive material, certain detailed design drawings, information on nearby facilities, emergency planning information, and certain assessments of vulnerability and safety analyses.
OCCMTO	Ocean Common Carrier and Marine Terminal Operator Agreements. Relating to agreements between or among ocean common carriers and marine terminal operators as referenced in 46 USC 40301 and 40306.
SERV	Ocean Common Carrier Service Contracts. Relating to an agreement for the provision of services filed with the Federal Maritime Commission as referenced in 46 USC 40502(b), 46 CFR 530.4, and/or 46 CFR 531.4(a).
CUI-PROVISIONAL-OSI	Provisional - Operations Security Information. Unclassified information that could constitute an indicator of U.S. Government intentions, capabilities, operations, or activities or otherwise threaten/compromise operations security.
APP	Patent Applications. Application for patent filed under 35 U.S.C. 111(a) that includes all types of patent applications (i.e., utility, design, plant, and reissue) except provisional applications. The nonprovisional application establishes the filing date and initiates the examination process. A nonprovisional utility patent application must include a specification, including a claim or claims; drawings, when necessary; an oath or declaration; and the prescribed filing fee.
TRACE	Pen Register/Trap & Trace. Related to devices used to identify incoming and outgoing telephone numbers.
RESD	Permanent Resident Status. Related to applications and associated hearings to grant permanent residency to foreign nationals living in the United States.
PERS	Personnel Records. Related to the employees of federal agencies.
CUI-PROVISIONAL-PSI	Provisional - Personnel Security Information. Information that could result in physical risk to DHS personnel or other individuals that DHS is responsible for protecting.
PEST	Pesticide Producer Survey. Related to the data gathered regarding the production of pesticides that specifies the non-disclosure of the identity and location of individual producers.
PHYS	Physical Security. Related to protection of federal buildings, grounds or property.

CVEnumISMCUIBasic Values	
Value	Documentation
CUI-PROVISIONAL-PHYSH	Provisional - Physical Security - Homeland. Assessments or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of federal buildings, grounds, or property, such as threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation.
PRE	Presentence Report. A report, generally prepared to assist the court in determining the most appropriate sentence for a defendant. It can include an assessment of the nature and seriousness of the offense and should contain details summarizing the background information of the defendant and the crime.
PRIOR	Prior Arrest. Information related to previous instances of law enforcement official's apprehension and formal processing of a suspect.
CUI-PROVISIONAL-PRIVACY	Provisional - Privacy Information. Information referred to as Personally Identifiable Information (PII). PII embodies information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
POST	Proprietary Postal. Concerning or related to the course of business of the United States Postal Service.
LPROT	Protective Order. Stipulation that certain information that would normally fall under discovery rules will not be disclosed for specifically stated reason.
RAIL	Railroad Safety Analysis Records. Related to the establishment, implementation, or modification of a railroad safety risk reduction program or pilot program, if the record is: (1) Supplied to the Secretary (of Transportation) pursuant to that safety risk reduction program or pilot program; or (2) made available for inspection and copying by an officer, employee, or agent of the Secretary pursuant to that safety risk reduction program or pilot program.
RTR	Retirement. Related to post-employment funding provided by an employer.
RWRD	Reward. Related to the identity of a recipient of a reward.

CVEnumISMCUIBasic Values	
Value	Documentation
SAFE	SAFETY Act Information. Defined as "SAFETY Act Confidential Information" in 6 CFR Part 25, the regulations implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, SAFETY Act Information includes any and all information and data voluntarily submitted to the Department of Homeland Security under this part (including Applications, Pre-Applications, other forms, supporting documents and other materials relating to any of the foregoing, and responses to requests for additional information), including, but not limited to, inventions, devices, Technology, know-how, designs, copyrighted information, trade secrets, confidential business information, analyses, test and evaluation results, manuals, videotapes, contracts, letters, facsimile transmissions, electronic mail and other correspondence, financial information and projections, actuarial calculations, liability estimates, insurance quotations, and business and marketing plans.
PSEC	Secrecy Orders. An order by the Commissioner of Patents that an invention be kept secret and to withhold the publication of an application or the grant of a patent due to national security concerns.
CUI-PROVISIONAL-PII	Provisional - Sensitive Personally Identifiable Information. A subset of PII that, if lost, compromised or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. a. Examples of stand-alone PII include: Social Security Numbers (SSN), driver's license or state identification number; Alien Registration Numbers; financial account number; and biometric identifiers such as fingerprint, voiceprint, or iris scan. b. Additional examples of SPII include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements: Truncated SSN (such as last four digits) Date of birth (month, day, and year) Citizenship or immigration status Ethnic or religious affiliation Sexual orientation Criminal history Medical information System authentication information such as mother's maiden name, account passwords, or personal identification numbers c. Other PII may be "sensitive" depending on its context, such in as a list of employees and their performance rating(s) or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII, but is not sensitive.
SCV	Sex Crime Victim. Related to the identity of a victim of a sex offense.
SBIZ	Small Business Research and Technology. Relating to certain "Small Business Innovation Research Program" and "Small Business Technology Transfer Program" information in a government database, as referenced in 15 USC 638(k)(2).

<b>CVEnumISMCUIBasic Values</b>	
<b>Value</b>	<b>Documentation</b>
SSEL	Source Selection. Per FAR 2.101: any of the following information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly: (Items 1-10).
STAT	Statistical Information. Refers to information collected by a Federal statistical agency, unit, or program for statistical purposes or used for statistical activities; under law, regulation, or Government-wide policy such 'Statistical' CUI requires: (1) protection from unauthorized disclosure; (2) special handling safeguards; and/or (3) prescribed limits on access or dissemination.
ADJ	Status Adjustment. Related to applications for the adjustment of immigration status.
STUD	Student Records. As per 20 USC 1232g, the Family Educational Rights and Privacy Act of 1974, an education record which is comprised of those records which are directly related to a student.
CONREG	System for Award Management. Relating to the primary United States Government system for contractor registration and awards.
CONV	Tax Convention. Related to any-- (A) agreement entered into with the competent authority of one or more foreign governments pursuant to a tax convention, (B) application for relief under a tax convention, (C) background information related to such agreement or application, (D) document implementing such agreement, and (E) other information exchanged pursuant to a tax convention which is treated as confidential or secret under the tax convention. Tax convention information originating with the IRS generally retains its confidential status even when it resides with agencies other than the IRS.
TAI	Taxpayer Advocate Information. A local taxpayer advocate (LTA) has the discretion to not disclose to the IRS contact with, or information provided by, a taxpayer. Such discretion may result in declinations of requests for information by IRS personnel including cases involving criminal tax investigations or those where the failure to provide information to the IRS would be beneficial to the taxpayer but to the detriment of the IRS. Such discretion does not extend to cases where the LTA believes a taxpayer is using the Taxpayer Advocate's office to perpetuate a fraud on the government or in cases where the information is sought in litigation.
PROT	Temporary Protected Status. Related to findings that conditions in a given country pose a danger to personal safety due to ongoing armed conflict or an environmental disaster and persons should receive special temporary status to remain in the United States.
LSCRN	Terrorist Screening. Related to information gathering and analysis concerning possible threats or acts of a destructive nature.

<b>CVEnumISMCUIBasic Values</b>	
<b>Value</b>	<b>Documentation</b>
DCNI	Unclassified Controlled Nuclear Information - Defense. Relating to Department of Defense special nuclear material (SNM), equipment, and facilities, as defined by 32 CFR 223.
UCNI	Unclassified Controlled Nuclear Information - Energy. Relating to certain design and security information concerning nuclear facilities, materials, and weapons, specific to the Department of Energy.
LVIC	Victim. Information requiring protection of the name or other details that may identify one who was the victim of a crime.
IVIC	Victims of Human Trafficking. Related to identifiable information of persons who have been victims of human trafficking and their family members.
VISA	Visas. Related to applications or permits to enter the United States.
WATER	Water Assessments. Vulnerability Assessments on the risks and security of public drinking water systems, to include, but not be limited to, a review of pipes and constructed conveyances, physical barriers, water collection, pretreatment, treatment, storage and distribution facilities, electronic, computer or other automated systems which are utilized by the public water system, the use, storage, or handling of various chemicals, and the operation and maintenance of such system.
WHSTL	Whistleblower Identity. Identity of anyone providing information relating to a legal violation or illicit or unsafe activity, including information provided by a whistleblower which could reasonably be expected to reveal the identity of a whistleblower.
WIT	Witness Protection. Information related to the secretive details associated with one who has testified or may testify under circumstances that require secrecy of that individual and details pertaining to that person.

## Chapter 8 - CVEnumISMUISpecified for ISM

### 8.1 - Descriptive information

- Description: All currently valid CUI Specified markings from the National Archives. This CVE is used by @ism:cuiSpecified.
- Multiplicity: Multi-Valued Max Values: 57
- URN: urn:us:gov:ic:cvenum:ism:cuispecified
- Created: 2019-08-16T16:14:00-05:00
- Source: National Archives CUI Category Markings
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 8.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMUISpecified.xml

**Table 8 - CVEnumISMUISpecified Values**

CVEnumISMUISpecified Values	
Value	Documentation
AIV	Accident Investigation. Related to information obtained during the course of an accident or incident investigation. Including but not limited to information related to wreckage, records, mail, or cargo.
ADPO	Administrative Proceedings. Adjudication of agency-related matters including, but not limited to, dispute resolution, settlements, and issuances of orders.
CRITAN	Ammonium Nitrate. Related to registration information of those who own and operate ammonium nitrate facilities, purchasers of ammonium nitrate, and the regulation of sales and transfers of ammonium nitrate.
ARCHR	Archaeological Resources. Related to information about the nature and location of any archaeological resource for which the excavation or removal requires a permit or other permission.

CVEnumISMCUISpecified Values	
Value	Documentation
FSEC	Bank Secrecy. Information that is provided to the government pursuant to the Bank Secrecy Act, including but not limited to, suspicious activity reports (SAR), currency transaction reports (CTR), reports of international transportation of currency or monetary instruments (CMIR), reports of cash payment over \$10,000 received in trade or business, and reports of foreign bank and financial accounts (FBAR). Reports filed under the Bank Secrecy Act (BSA), codified in relevant part at 31 U.S.C. § 5311 et seq, are specifically exempt from disclosure under the Freedom of Information Act, codified at 5 U.S.C. § 552, and also may not be disclosed under any State, local, tribal, or territorial “freedom of information,” “open government,” or similar law. See 31 U.S.C. § 5319; 5 U.S.C. § 552(b)(3). These reports (BSA Reports), are maintained in a system of records containing information compiled for law enforcement investigative purposes that has been exempted from the access provisions of the Privacy Act in accordance with 5 U.S.C. §§ 552a(j)(2) and (k)(2). BSA Reports may only be re-disseminated in strict accordance with guidelines established by the Financial Crimes Enforcement Network (FinCEN), the Treasury bureau that administers the BSA. Suspicious Activity Reports, one of the types of required reports filed under the BSA, are required to be kept confidential in accordance with 31 U.S.C. § 5318(g)(2) and implementing regulations. To the extent information falling under the purview of the BSA is collected, accessed, or used for any Federal tax administration purpose, it is also subject to the confidentiality provisions of the Internal Revenue Code, codified at 26 U.S.C. § 6103.
BUDG	Budget. Related to information concerning the federal budget, including authorizations and estimates of income and expenditures.
FUND	Campaign Funds. Related to information obtained in connection to an investigation into campaign finance and disclosure laws. Usage may include but is not limited to notification or investigation pertaining to financial support of a candidate for election.
CVI	Chemical-terrorism Vulnerability Information. In accordance with Section 550(c) of the Department of Homeland Security Appropriations Act of 2007, the following information, whether transmitted verbally, electronically, or in written form, shall constitute CVI, see (1) - (9).

CVEnumISMCUISpecified Values	
Value	Documentation
CHLD	Child Pornography. From 18 USC 2256(8) "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where— (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct
CCI	Consumer Complaint Information. Related to information concerning consumer complaints or inquiries concerning financial institutions or consumer financial products and services, and responses to them.
CONTRACT	Contract Use. Stipulations for a contractor to meet before material may be used in performance of certain contracts.
SUB	Controlled Substances. Information obtained by the Drug Enforcement Administration (DEA) or in DEA investigative reports related to controlled substances.
CTI	Controlled Technical Information. Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
CHRI	Criminal History Records Information. Related to information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release.

<b>CVEnumISMCUISpecified Values</b>	
<b>Value</b>	<b>Documentation</b>
CEII	Critical Energy Infrastructure Information. Critical energy infrastructure information means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: (i) Relates details about the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure;... and (iii) Does not simply give the general location of the critical infrastructure.
LDNA	DNA. Related to hereditary material in humans that is used for law enforcement purposes.
EXPT	Export Controlled. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.
JURY	Federal Grand Jury. Material obtained pursuant to a federal grand jury subpoena, which includes (1) any reference to a specific sitting grand jury; (2) any documentation or data obtained by a grand jury subpoena if disclosure of such material tends to reveal what transpired before or at the direction of the federal grand jury; (3) documentation prepared specifically for the federal grand jury; and (4) transcripts or other recordings of testimony presented to the federal grand jury.
TAX	Federal Taxpayer Information. Related to returns and return information which are submitted, gathered or generated in conjunction with taxpayers' responsibilities to comply with federal tax provisions in the United States Code. "Returns" includes information that is provided to the government pursuant to Title 26, including tax or information returns, declarations of estimated tax or claims for refund. "Return information" includes a taxpayer's identity, the nature, source or amount of income or any information received by, recorded by, prepared by or furnished to Internal Revenue Service relevant to the determination of tax liability including whether the taxpayer is the subject of investigation. This protection extends to such items as medical, financial and other personal information submitted to the IRS by taxpayers. Standards (typically tolerances, audit criteria and law enforcement techniques) related to the selection of returns for examination should only be disclosed to the extent their disclosure would not impair assessment, collection or enforcement under the internal revenue laws. Tax data originating with the IRS generally retains its confidential status even when it resides with agencies other than the IRS.

CVEnumISMCUISpecified Values	
Value	Documentation
FISA	Foreign Intelligence Surveillance Act. Related to unclassified and declassified information that is collected from unconsenting individuals under the authority of the Foreign Intelligence Surveillance Act (FISA).
FISAB	Foreign Intelligence Surveillance Act Business Records. Related to books, records, papers, documents, and other items produced for an investigation to obtain foreign intelligence information.
FNC	General Financial Information. Related to the duties, transactions, or otherwise falling under the purview of financial institutions or United States Government fiscal functions. Uses may include, but are not limited to, customer information held by a financial institution.
INTEL	General Intelligence. Related to intelligence activities, sources, or methods.
NUC	General Nuclear. Related to protection of information concerning nuclear reactors, materials, or security.
PRVCY	General Privacy. Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-17-12, or "means of identification" as defined in 18 USC 1028(d)(7).
PROCURE	General Procurement and Acquisition. Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.
PROPIN	General Proprietary Business Information. Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.
GENETIC	Genetic Information. The term "genetic information" means, with respect to any individual, information about-- (i) such individual's genetic tests, (ii) the genetic tests of family members of such individual, and (iii) the manifestation of a disease or disorder in family members of such individual.
GEO	Geodetic Product Information. Related to imagery, imagery intelligence, or geospatial information.

<b>CVEnumISMCUISpecified Values</b>	
<b>Value</b>	<b>Documentation</b>
HLTH	Health Information. As per 42 USC 1320d(4), "health information" means any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
HISTP	Historic Properties. Related to the location, character, or ownership of historic property.
INF	Informant. Related to the identity of a human source.
PRIIG	Inspector General Protected. Related to the identity of a person making a report to the Inspector General of any Executive agency.
IFNC	Intelligence Financial Records. Related to financial records obtained for intelligence or counterintelligence activity, investigation, or analysis.
ID	Internal Data. Refers to a category of information that is not intended to be disseminated beyond CIA channels that involves intelligence activities, sources, or methods. This information may also relate to the CIA's organization, functions, names, official titles, salaries, or numbers of personnel.
INTL	International Agreement Information. Information provided by, otherwise made available by, or produced in cooperation with, a foreign government or international organization that requires protection pursuant to an existing treaty, agreement, bilateral exchange or other obligation under the requirements stipulated in 10 USC 130c(b), when not subject to classification under Executive Order 13526. Title 10 USC 130c(b) may exempt this class of foreign government information from the safeguard provisions otherwise required by Executive Order 13526. Per Title 10 USC 130c(h) the following national security officials are the only ones defined by statute as able to determine such information requires control: (A) The Secretary of Defense, with respect to information of concern to the Department of Defense. (B) The Secretary of Homeland Security, with respect to information of concern to the Coast Guard, as determined by the Secretary, but only while the Coast Guard is not operating as a service in the Navy. (C) The Secretary of Energy, with respect to information concerning the national security programs of the Department of Energy, as determined by the Secretary.
INV	Investigation. Related to information obtained during the course of a law enforcement investigation or action, civil or criminal.

<b>CVEnumISMCUISpecified Values</b>	
<b>Value</b>	<b>Documentation</b>
LFNC	Law Enforcement Financial Records. Related to financial records obtained for law enforcement purposes.
NPSR	National Park System Resources. Related to information concerning the nature and specific location of a National Park System resource that is endangered, threatened, rare, or commercially valuable, of mineral or paleontological objects within System units, or of objects of cultural patrimony within System units.
NNPI	Naval Nuclear Propulsion Information. Related to the safety of reactors and associated naval nuclear propulsion plants, and control of radiation and radioactivity associated with naval nuclear propulsion activities, including prescribing and enforcing standards and regulations for these areas as they affect the environment and the safety and health of workers, operators, and the general public.
SRI	Nuclear Security-Related Information. Related to information that could be useful, or could reasonably be expected to be useful, to a terrorist in a potential attack that does not qualify as Safeguards or classified information, including the exact location and quantities of radioactive material, certain detailed design drawings, information on nearby facilities, emergency planning information, and certain assessments of vulnerability and safety analyses.
PERS	Personnel Records. Related to the employees of federal agencies.
MFC	Proprietary Manufacturer. Relating to the production of a consumer product to include that of a private labeler.
PCII	Protected Critical Infrastructure Information. As defined by 6 USC 131-134, and 6 CFR 29, PCII relates to threats, vulnerabilities, or operational experience related to the national infrastructure. PCII offers protection to private sector infrastructure information voluntarily shared with government entities for purposes of homeland security.
LPROT	Protective Order. Stipulation that certain information that would normally fall under discovery rules will not be disclosed for specifically stated reason.
SGI	Safeguards Information. Pursuant to 42 USC 2011, et seq., and as defined in 10 CFR 73.2, SGI relates to security related information concerning the physical protection of source, byproduct or special nuclear material and the detailed security measures for facilities and information contained within security plans.

CVEnumISMCUISpecified Values	
Value	Documentation
SSI	Sensitive Security Information. As defined in 49 C.F.R. Part 15.5, Sensitive Security Information is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DOT has determined would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to transportation safety. As defined in 49 C.F.R. Part 1520.5, Sensitive Security Information is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DHS/TSA has determined would, among other things, be detrimental to the security of transportation.
SSEL	Source Selection. Per FAR 2.101: any of the following information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly: (Items 1-10).
STAT	Statistical Information. Refers to information collected by a Federal statistical agency, unit, or program for statistical purposes or used for statistical activities; under law, regulation, or Government-wide policy such 'Statistical' CUI requires: (1) protection from unauthorized disclosure; (2) special handling safeguards; and/or (3) prescribed limits on access or dissemination.
STUD	Student Records. As per 20 USC 1232g, the Family Educational Rights and Privacy Act of 1974, an education record which is comprised of those records which are directly related to a student.
TSCA	Toxic Substances. Health, safety, and exposure information related to chemical substances, chemical mixtures, and articles as defined under the Toxic Substances Control Act (TSCA).
DCNI	Unclassified Controlled Nuclear Information - Defense. Relating to Department of Defense special nuclear material (SNM), equipment, and facilities, as defined by 32 CFR 223.
UCNI	Unclassified Controlled Nuclear Information - Energy. Relating to certain design and security information concerning nuclear facilities, materials, and weapons, specific to the Department of Energy.
CENS	US Census. Related to information gathered by the Bureau of the Census during the process of collecting, compiling, evaluating, analyzing of demographic, economic, and social data pertaining at a specified time to any or all persons in the United States and dissemination is limited to those with special sworn status, who may only use the data for statistical purposes and only for those statistical purposes for which the data was supplied.

<b>CVEnumISMCIUSpecified Values</b>	
<b>Value</b>	<b>Documentation</b>
WHSTL	Whistleblower Identity. Identity of anyone providing information relating to a legal violation or illicit or unsafe activity, including information provided by a whistleblower which could reasonably be expected to reveal the identity of a whistleblower.
WIT	Witness Protection. Information related to the secretive details associated with one who has testified or may testify under circumstances that require secrecy of that individual and details pertaining to that person.
WDT	Written Determinations. Rulings, determination letters, technical advice memoranda or Chief Counsel Advice, as those terms are defined in Treasury Regulation 301.6110-2, which are made available for public inspection subject to the withholding of certain types of data as enumerated in Treasury Regulation 301-6110.

## Chapter 9 - CVEnumISMDissem for ISM

### 9.1 - Descriptive information

- Description: All currently valid Dissemination controls from the published IC Register and Manual (ICRM), followed by the DOD WAIVED dissemination control from DOD-5205-07-SAP, followed by the ISOO limited set of CUI dissemination controls. This CVE template is used to produce CVEnumISM dissem CVEs for @ism:disseminationControls. This CVE template is mainly used to provide all the dissemination controls across ICRM and CUI contexts, for use as a schema fragment in the CVEGenerated folder of ISM.
- Multiplicity: Multi-Valued Max Values: 22
- URN: urn:us:gov:ic:cvenum:ism:dissem
- Created: 2023-06-09T19:40:39.525Z
- Source: 1) IC Systems Register and Manual; 2) ISOO CUI Register
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 9.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMDissem.xml

**Table 9 - CVEnumISMDissem Values**

CVEnumISMDissem Values	
Value	Documentation
RS	RISK SENSITIVE
FOUO	FOR OFFICIAL USE ONLY
OC	ORIGINATOR CONTROLLED
OC-USGOV	ORIGINATOR CONTROLLED US GOVERNMENT
IMC	CONTROLLED IMAGERY
NF	NOT RELEASABLE TO FOREIGN NATIONALS
PR	CAUTION-PROPRIETARY INFORMATION INVOLVED
REL	AUTHORIZED FOR RELEASE TO
RELIDO	RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL
EYES	EYES ONLY
DSEN	DEA SENSITIVE
RAWFISA	RAW FOREIGN INTELLIGENCE SURVEILLANCE ACT
FISA	FOREIGN INTELLIGENCE SURVEILLANCE ACT
DISPLAYONLY	AUTHORIZED FOR DISPLAY BUT NOT RELEASE TO

<b>CVEnumISMDissem Values</b>	
<b>Value</b>	<b>Documentation</b>
EXEMPT_FROM_ICD501_DISCOVERY	EXEMPT FROM ICD501 DISCOVERY
WAIVED	WAIVED
AC	Attorney-Client
AWP	Attorney-WP
DL_ONLY	DL ONLY
FED_ONLY	FED ONLY
FEDCON	FEDCON
NOCON	NOCON

## Chapter 10 - CVEnumISMDissemCommingled for ISM

### 10.1 - Descriptive information

- Description: Dummy Template file to work with the automated build process. The CVEnumISMDissemCommingled.xml and .xsd files are built by the CVEnumISMDissemCommingled.xsl transformation stylesheet from CVEnumISMDissem\_Template.xml, CVEnumISMDissemIcrmNotInCommingled\_Template.xml, CVEnumISMDissemCui\_Template.xml, and CVEnumISMDissemCommon\_Template.xml
- Multiplicity: Multi-Valued Max Values: 21
- URN: urn:us:gov:ic:cvenum:ism:dissem:commingled
- Created: 2023-06-09T19:40:40.113Z
- Source: 1) IC Systems Register and Manual; 2) ISOO CUI Register
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 10.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMDissemCommingled.xml

**Table 10 - CVEnumISMDissemCommingled Values**

CVEnumISMDissemCommingled Values	
Value	Documentation
RS	RISK SENSITIVE
OC	ORIGINATOR CONTROLLED
OC-USGOV	ORIGINATOR CONTROLLED US GOVERNMENT
IMC	CONTROLLED IMAGERY
NF	NOT RELEASABLE TO FOREIGN NATIONALS
PR	CAUTION-PROPRIETARY INFORMATION INVOLVED
REL	AUTHORIZED FOR RELEASE TO
RELIDO	RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL
EYES	EYES ONLY
DSEN	DEA SENSITIVE
RAWFISA	RAW FOREIGN INTELLIGENCE SURVEILLANCE ACT
FISA	FOREIGN INTELLIGENCE SURVEILLANCE ACT
DISPLAYONLY	AUTHORIZED FOR DISPLAY BUT NOT RELEASE TO
EXEMPT_FROM_ICD501 _DISCOVERY	EXEMPT FROM ICD501 DISCOVERY

CVEnumISMDissemCommingle Values	
Value	Documentation
WAIVED	WAIVED
AC	Attorney-Client
AWP	Attorney-WP
DL_ONLY	DL ONLY
FED_ONLY	FED ONLY
FEDCON	FEDCON
NOCON	NOCON

## Chapter 11 - CVEnumISMDissemCui for ISM

### 11.1 - Descriptive information

- Description: Currently valid Dissemination controls for use with Controlled Unclassified Information (CUI), from the ISOO limited set of CUI dissemination controls. The CVE template CVEnumISMDissemCui\_Template is used to create a Dissem CVE used for pure Controlled Unclassified Information (CUI). This is CVEnumISMDissemCui. It contains only dissemination controls published in the ISOO CUI Register. This template supports a straight copy to create CVEnumISMDissemCui.
- Multiplicity: Multi-Valued Max Values: 11
- URN: urn:us:gov:ic:cvenum:ism:dissem:cui
- Created: 2023-06-09T19:40:40.773Z
- Source: 1) IC Systems Register and Manual; 2) ISOO CUI Register
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 11.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMDissemCui.xml

**Table 11 - CVEnumISMDissemCui Values**

CVEnumISMDissemCui Values	
Value	Documentation
AC	Attorney-Client
AWP	Attorney-WP
DISPLAYONLY	AUTHORIZED FOR DISPLAY BUT NOT RELEASE TO
DL_ONLY	DL ONLY
EXEMPT_FROM_ICD501_DISCOVERY	EXEMPT FROM ICD501 DISCOVERY
FED_ONLY	FED ONLY
FEDCON	FEDCON
NF	NOT RELEASABLE TO FOREIGN NATIONALS
NOCON	NOCON
REL	AUTHORIZED FOR RELEASE TO
RELIDO	RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL

## Chapter 12 - CVEnumISMDissemlcrm for ISM

### 12.1 - Descriptive information

- Description: All currently valid Dissemination controls from the published IC Markings System Register and Manual (acronym ICRM), followed by the DOD WAIVED dissemination control from DOD-5205-07-SAP. This CVE template is used to produce CVEnumISMDissemlcrm.xml for @ism:disseminationControls.
- Multiplicity: Multi-Valued Max Values: 16
- URN: urn:us:gov:ic:cvenum:ism:dissem:icrm
- Created: 2023-06-09T19:40:41.335Z
- Source: 1) IC Systems Register and Manual
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 12.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMDissemlcrm.xml

**Table 12 - CVEnumISMDissemlcrm Values**

CVEnumISMDissemlcrm Values	
Value	Documentation
RS	RISK SENSITIVE
FOUO	FOR OFFICIAL USE ONLY
OC	ORIGINATOR CONTROLLED
OC-USGOV	ORIGINATOR CONTROLLED US GOVERNMENT
IMC	CONTROLLED IMAGERY
NF	NOT RELEASABLE TO FOREIGN NATIONALS
PR	CAUTION-PROPRIETARY INFORMATION INVOLVED
REL	AUTHORIZED FOR RELEASE TO
RELIDO	RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL
EYES	EYES ONLY
DSEN	DEA SENSITIVE
RAWFISA	RAW FOREIGN INTELLIGENCE SURVEILLANCE ACT
FISA	FOREIGN INTELLIGENCE SURVEILLANCE ACT
DISPLAYONLY	AUTHORIZED FOR DISPLAY BUT NOT RELEASE TO
EXEMPT_FROM_ICD501 _DISCOVERY	EXEMPT FROM ICD501 DISCOVERY
WAIVED	WAIVED

## Chapter 13 - CVEnumISMElements for ISM

### 13.1 - Descriptive information

- Description: All currently authorized ISM element names.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:ism:elements
- Created: 2011-04-15T15:16:00-05:00
- Source: ISM schema
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 13.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMElements.xml

**Table 13 - CVEnumISMElements Values**

CVEnumISMElements Values	
Value	Documentation
Notice	Notice element
NoticeText	NoticeText element
NoticeList	NoticeList element
NoticeExternal	NoticeExternal element
NoticeExternalList	NoticeExternalList element

## Chapter 14 - CVEnumISMExemptFrom for ISM

### 14.1 - Descriptive information

- Description: Current rule set names that documents may comply with. This CVE is used by @ism:exemptFrom.
- Multiplicity: Multi-Valued Max Values: 2
- URN: urn:us:gov:ic:cvenum:ism:exemptfrom
- Created: 2010-05-30T16:52:00-04:00
- Source: ISM schema
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 14.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMExemptFrom.xml

**Table 14 - CVEnumISMExemptFrom Values**

CVEnumISMExemptFrom Values	
Value	Documentation
IC_710_MANDATORY_FD DR	Document claims exemption from ICD-710 rules mandating the use of Foreign Disclosure and Release markings that have been encoded in ISM. Currently, the requirement for FD&R is only mandatory for Disseminated Analytic Product; however, it is strongly encouraged otherwise.
DOD_DISTRO_STATEM ENT	Document claims exemption from the rules in DoD5230.24 requiring DoD Distribution Statements that have been encoded into ISM.

## Chapter 15 - CVEnumISMHighWaterNATO for ISM

### 15.1 - Descriptive information

- Description: The highest classification of any portion that has either @ism:ownerProducer contains NATO or @FGIsourceOpen contains NATO. The @ism:highWaterNATO attribute will be compared against an entity's fineAccessControls NATO value.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:ism:HighWaterNATO
- Created: 2012-01-04T00:14:00-04:00
- Source: IC Systems Register and Manual
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 15.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMHighWaterNATO.xml

**Table 15 - CVEnumISMHighWaterNATO Values**

CVEnumISMHighWaterNATO Values	
Value	Documentation
NATO-U	NATO UNCLASSIFIED
NATO-R	NATO RESTRICTED
NATO-C	NATO CONFIDENTIAL
NATO-S	NATO SECRET
NATO-TS	NATO TOP SECRET

## Chapter 16 - CVEnumISMNonIC for ISM

### 16.1 - Descriptive information

- Description: All currently valid Non-IC markings from the published register. This CVE is used by @ism:nonICmarkings.
- Multiplicity: Multi-Valued Max Values: 9
- URN: urn:us:gov:ic:cvenum:ism:nonic
- Created: 2012-01-04T00:14:00-04:00
- Source: IC Systems Register and Manual
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 16.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMNonIC.xml

**Table 16 - CVEnumISMNonIC Values**

CVEnumISMNonIC Values	
Value	Documentation
DS	LIMITED DISTRIBUTION
XD	EXCLUSIVE DISTRIBUTION
ND	NO DISTRIBUTION
SBU	SENSITIVE BUT UNCLASSIFIED
SBU-NF	SENSITIVE BUT UNCLASSIFIED NOFORN
LES	LAW ENFORCEMENT SENSITIVE
LES-NF	LAW ENFORCEMENT SENSITIVE NOFORN
SSI	SENSITIVE SECURITY INFORMATION
NNPI	NAVAL NUCLEAR PROPULSION INFORMATION

## Chapter 17 - CVEnumISMNonUSControls for ISM

### 17.1 - Descriptive information

- Description: NonUS Control markings supported by ISM. This CVE is used by @ism:nonUSControls.
- Multiplicity: Multi-Valued Max Values: 3
- URN: urn:us:gov:ic:cvenum:ism:nonuscontrols
- Created: 2010-06-06T20:11:00-04:00
- Source: ISM schema
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 17.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMNonUSControls.xml

**Table 17 - CVEnumISMNonUSControls Values**

CVEnumISMNonUSControls Values	
Value	Documentation
NATO-ATOMAL	NATO Atomal mark
NATO-BOHEMIA	NATO Bohemia mark
NATO-BALK	NATO Balk mark

## Chapter 18 - CVEnumISMNotice for ISM

### 18.1 - Descriptive information

- Description: All currently authorized Notice values. This CVE is used by @ism:noticeType.
- Multiplicity: Multi-Valued Max Values: 27
- URN: urn:us:gov:ic:cvenum:ism:notice
- Created: 2010-03-12T11:29:00-04:00
- Source: DoD Instruction 5200.01; ISOO 32 CFR Parts 2001 and 2003; DoD Instruction 5230.24
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 18.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMNotice.xml

**Table 18 - CVEnumISMNotice Values**

CVEnumISMNotice Values	
Value	Documentation
FISA	FISA Warning statement
RAWFISA	RAWFISA Warning statement
IMC	IMCON Warning statement
CNWDI	Controlled Nuclear Weapon Design Information Warning statement
RD	RD Warning statement
FRD	FRD Warning statement
DS	LIMDIS caveat
LES	LES Notice
LES-NF	LES-NF Notice
DSEN	DSEN Notice
DoD-Dist-A	DoD Distribution statement A from DoD Directive 5230.24
DoD-Dist-B	DoD Distribution statement B from DoD Directive 5230.24
DoD-Dist-C	DoD Distribution statement C from DoD Directive 5230.24
DoD-Dist-D	DoD Distribution statement D from DoD Directive 5230.24
DoD-Dist-E	DoD Distribution statement E from DoD Directive 5230.24
DoD-Dist-F	DoD Distribution statement F from DoD Directive 5230.24
US-Person	US Person info Notice

<b>CVEnumISMNotice Values</b>	
<b>Value</b>	<b>Documentation</b>
pre13526ORCON	Indicates that an instance document must abide by rules pertaining to ORIGINATOR CONTROLLED data issued prior to Executive Order 13526.
POC	Indicates that the contents of this notice specify the contact information for a required point-of-contact.
COMSEC	COMSEC Notice
SSI	Indicates that this is the notice for Sensitive Security Information
RSEN	Risk Sensitive Notice
IMCON_RSEN	Indicates SAT warning statements include IMCON and RSEN markings
GEOCAP	GEOCAP Warning statement
NATO	NATO Warning statement
RC_Dissemination_Control_Required	This product was collected in a restricted collection mode. Redaction, chipping and release determination shall not result in more permissive release than NOFORN regardless of the Security Indicator Codes (SIC) associated with the product
ITAR-EAR	Warning statement for International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) in accordance with DoD 5230.24, Distribution Statements on Technical Documents.

## Chapter 19 - CVEnumISMNoticeProse for ISM

### 19.1 - Descriptive information

- Description: All currently authorized notice prose values in support of out-of-band notices. This CVE is used by @ism:noticeProseID.
- Multiplicity: Multi-Valued Max Values: 21
- URN: urn:us:gov:ic:cvenum:ism:noticeprose
- Created: 2023-06-09T19:40:41.924Z
- Source: IC Systems Register and Manual; DoD Instruction 5230.24; DoD Manual 5200.01; CMT
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 19.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMNoticeProse.xml

**Table 19 - CVEnumISMNoticeProse Values**

CVEnumISMNoticeProse Values	
Value	Documentation
FISA_00001	CIA Special Procedures FISA: This dissemination includes FBI information from FBI FISA collection. Such information, and any information derived therefrom, may only be used in a US legal or administrative proceeding with the advance authorization of the Attorney General. Any recipient interested in obtaining authorization for such use in a US legal or administrative proceeding should contact FBI Headquarters. Any further dissemination outside of intelligence channels and/or for law enforcement purposes must be made through FBI Headquarters. Any reproduction, dissemination, or communication (including, but not limited to oral briefings) of this information must be accompanied by a statement of these restrictions.
FISA_00002	FBI Minimized FISA: This report includes information from FBI FISA collection. Such information, and any information derived therefrom, may only be used in a US legal or administrative proceeding with the advance authorization of the Attorney General. Any recipient interested in obtaining authorization for such use in a US legal or administrative proceeding should contact FBI Headquarters. Any further dissemination outside of intelligence channels and/or for law enforcement purposes must be made through FBI Headquarters. Any reproduction, dissemination, or communication (including, but not limited to oral briefings) of this information must be accompanied by a statement of these restrictions.

CVEnumISMNoticeProse Values	
Value	Documentation
FISA_00003	This report includes information from FISA collection. Such information, and any information derived therefrom, may NOT be used in a domestic or foreign legal, judicial, or administrative proceeding without the advance authorization of the Attorney General. Any recipient interested in obtaining authorization for such use should contact NCTC Operations Center on (571) 280- 6000 (STE III) or 931-6000 secure. Any reproduction, dissemination, or communication (including but not limited to oral briefings) of this information must be accompanied by a statement of these restrictions.
RAWFISA_00001	FBI RAWFISA: This report includes information from FBI FISA collection that has not been evaluated in accordance with minimization procedures (raw FISA-acquired information). FBI personnel with authorized access to raw FISA-acquired information may review, translate, copy, transcribe, analyze, summarize, and use the information contained herein only in accordance with relevant minimization procedures and internal FBI policies. If the raw FISA-acquired information contained herein is not accompanied by handling instructions, then the recipient, following his/her review of the information, must either return the information to the sender of the information or destroy the information, unless the recipient determines the information meets the minimization standard. Once raw FISA-acquired information, and any information derived therefrom, has been minimized by FBI personnel, such minimized FISA-acquired information may only be used in a U.S. legal or administrative proceeding with the advance authorization of the Attorney General, and in coordination with FBI Headquarters.
CNWDI_00001	Critical Nuclear Weapons Design Information - DoD Instruction 5210.02 applies.
RD_00001	RESTRICTED DATA: This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended. Unauthorized disclosure is subject to Administrative and Criminal Sanctions.
FRD_00001	FORMERLY RESTRICTED DATA: Unauthorized disclosure is subject to Administrative and Criminal Sanctions. Handle as RESTRICTED DATA in foreign dissemination. Section 144b, Atomic Energy Act of 1954.
DS_00001	Distribution authorized to DoD, IAW 10 U.S.C. Section 130 and Section 455. Release authorized to U.S. DoD contractors IAW 48 C.F.R. Section 252.245-7000. Refer other requests to: Headquarters, NGA, ATTN: Release Officer, Mail Stop S82-OIA, 7500 GEOINT Drive, Springfield, VA 22150. Destroy IAW DoDD 5030.59. Removal of this caveat is prohibited.

CVEnumISMNoticeProse Values	
Value	Documentation
DSEN_00001	This document is the property of the DEA and may be distributed within the Federal Government (and its contractors), and to US intelligence, law enforcement, and public safety or protection officials with a need to know. Distribution beyond these entities without DEA authorization is strictly prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. The use of information in this report is pre-approved for US government Intelligence Community products, including finished analytic products distributed to US Executive Branch departments/agencies. Cited portions must carry the same classification and controls, and readers of this report must hold all appropriate clearances. The information in this report may not be used in legal proceedings, for operational or intelligence collection activities, shared with foreign persons or agencies, entered into non-DEA databases for operational purposes or reproduced in additional formats unless express permission is granted by the DEA based on a written request submitted to dea.onsi@dea.ic.gov (Top Secret), dea.onsi@dea.usdoj.sgov.gov (Secret), or dea.onsi-dl@dea.usdoj.gov (Unclassified).
DoD-Dist-A_00001	DISTRIBUTION STATEMENT A. Approved for public release.
COMSEC_00001	COMSEC Material - Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance.
SSI_00001	Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need-to-know," as defined in 49 CFR 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 USC 552 and 49 CFR parts 15 and 1520.
GEOCAP_00001	WARNING STATEMENT: This document contains Geospatial Intelligence Controlled Access Program (GEOCAP) information and must adhere to established handling instructions. Contact the GEOCAP program office at (S) 579-3848 or TCS_Security@coe.ic.gov for additional guidance.
NATO_00001	This document contains COSMIC TOP SECRET information.
NATO_00002	This document contains NATO SECRET information.
NATO_00003	This document contains NATO CONFIDENTIAL information.
NATO_00004	This document contains NATO RESTRICTED information.
NATO_00005	This document contains NATO UNCLASSIFIED information.

CVEnumISMNoticeProse Values	
Value	Documentation
RC_Dissemination_Control_Required_00001	This product was collected in a restricted collection mode. Redaction, chipping and release determination shall not result in more permissive release than NOFORN regardless of the Security Indicator Codes (SIC) associated with the product.
ITAR-EAR_00001	WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.
DISPLAYONLY_00001	Derivative use of this DISPLAY ONLY or REL TO in conjunction with DISPLAY ONLY marked information into other products is prohibited without prior authorization from the originating agency. Disclosure of DISPLAY ONLY or REL TO in conjunction with DISPLAY ONLY information is not authorized for other purposes or for disclosure or release and disclosure to other countries, international organizations, or coalitions not specified in the banner line or portion marking. Removal of this caveat is required once authorization is received by the originating agency.

## Chapter 20 - CVEnumISMPocType for ISM

### 20.1 - Descriptive information

- Description: All currently authorized types for ISM-related points-of-contact. This CVE is used by @ism:pocType.
- Multiplicity: Multi-Valued Max Values: 6
- URN: urn:us:gov:ic:cvenum:ism:pocType
- Created: 2011-07-13T14:42:00-04:00
- Source: DoD Directive 5230.24; ICD-710; Originator Controlled Memo, March 11, 2011
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 20.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMPocType.xml

**Table 20 - CVEnumISMPocType Values**

CVEnumISMPocType Values	
Value	Documentation
ICD-710	Point-of-contact for an ICD-710 notice.
DoD-Dist-B	DoD Distribution statement B from DoD Directive 5230.24
DoD-Dist-C	DoD Distribution statement C from DoD Directive 5230.24
DoD-Dist-D	DoD Distribution statement D from DoD Directive 5230.24
DoD-Dist-E	DoD Distribution statement E from DoD Directive 5230.24
DoD-Dist-F	DoD Distribution statement F from DoD Directive 5230.24

## Chapter 21 - CVEnumISMSAR for ISM

### 21.1 - Descriptive information

- Description: All currently valid SAR markings from the published register and DoD SAPCO. This CVE is used by @ism:SARIdentifier.
- Multiplicity: Multi-Valued Max Values: 0
- URN: urn:us:gov:ic:cvenum:ism:sar
- Created: 2023-06-09T19:40:42.513Z
- Source: 1) IC Systems Register and Manual; 2) DoD SAPCO
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 21.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMSAR.xml

**Table 21 - CVEnumISMSAR Values**

CVEnumISMSAR Values	
Value	Documentation

## Chapter 22 - CVEnumISMSARAuthorities for ISM

### 22.1 - Descriptive information

- Description: E.O. 13526 Sec. 4.3. Special Access Programs states that only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. This CVE lists the agencies that are authorized to establish SAPs, which we are calling the Special Access Required (SAR) Authorities. The ISM encoding of SAP values uses the SAR Authorities values as part of a SAP value in @ism:SARIdentifier, because there is no central registry or requirement to deconflict names.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:ism:sar
- Created: 2021-06-28T11:29:00-04:00
- Source: E.O. 13526 Section 4.3
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 22.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMSARAuthorities.xml

**Table 22 - CVEnumISMSARAuthorities Values**

CVEnumISMSARAuthorities Values	
Value	Documentation
STATE	STATE
DOD	DOD
DOE	DOE
DHS	DHS
AG	AG
DNI	DNI

## Chapter 23 - CVEnumISMSCIControls for ISM

### 23.1 - Descriptive information

- Description: All currently valid SCI controls from the published register. This CVE is used by @ism:SCIcontrols.
- Multiplicity: Multi-Valued Max Values: 20
- URN: urn:us:gov:ic:cvenum:ism:scicontrols
- Created: 2023-06-09T19:40:43.113Z
- Source: IC Systems Register and Manual
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 23.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMSCIControls.xml

**Table 23 - CVEnumISMSCIControls Values**

CVEnumISMSCIControls Values	
Value	Documentation
BUR	BUR
BUR-BLG	BUR-BLG
BUR-DTP	BUR-DTP
BUR-WRG	BUR-WRG
HCS	HCS
HCS-O	HCS-O
HCS-P	HCS-P
HCS-X	HCS-X
KLM	KLAMATH
KLM-R	KLAMATH-R
MVL	MARVEL
RSV	RESERVE
SI	SPECIAL INTELLIGENCE
SI-EU	ECRU
SI-G	SI-GAMMA
SI-NK	NONBOOK
TK	TALENT KEYHOLE
TK-BLFH	BLUEFISH

<b>CVEnumISMSCIControls Values</b>	
<b>Value</b>	<b>Documentation</b>
TK-IDIT	IDITAROD
TK-KAND	KANDIK

## Chapter 24 - CVEnumISMSecondBannerLine for ISM

### 24.1 - Descriptive information

- Description: All currently valid markings that can appear in the second banner line. This CVE is used by @ism:secondBannerLine.
- Multiplicity: Multi-Valued Max Values: 6
- URN: urn:us:gov:ic:cvenum:ism:secondbannerline
- Created: 2019-12-23T18:44:00-04:00
- Source: Classification Management Tools (CMT)
- Point of contact:
  - Office IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 24.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumISMSecondBannerLine.xml

**Table 24 - CVEnumISMSecondBannerLine Values**

CVEnumISMSecondBannerLine Values	
Value	Documentation
ACPI	ATTORNEY-CLIENT PRIVILEGED INFO
AWP	ATTORNEY WORK PRODUCT
CUSPI	CONTENTS INCLUDE US PERSON INFORMATION
DPPD	DELIBERATIVE PROCESS PRIVILEGED DOCUMENT
HVCO	HANDLE VIA CHANNELS ONLY
SSS	SOURCE SELECTION SENSITIVE

## Chapter 25 - CVEnumNTKAccessPolicy for ISM

### 25.1 - Descriptive information

- Description: NTK access policy names. All NTK enterprise access policy URNs start with 'urn:us:gov:ic:aces:ntk:'. Values in this CVE correspond to the terminating portion of NTK access policy URNs.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:ntk:accesspolicy
- Created: 2010-05-30T16:52:00-04:00
- Source: NTK ACES
- Point of contact:
  - Office of the IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 25.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumNTKAccessPolicy.xml

**Table 25 - CVEnumNTKAccessPolicy Patterns**

CVEnumNTKAccessPolicy Values	
Pattern	Documentation
urn:us:gov:ic:aces:ntk:propin:([A-Za-z][A-Za-z0-9\-\_\.;(),:]+\{1,64})	Regex for extension of PROPIN with non-IC CIO access policy URN.

**Table 26 - CVEnumNTKAccessPolicy Values**

CVEnumNTKAccessPolicy Values	
Value	Documentation
urn:us:gov:ic:aces:ntk:xd	Exclusive Distribution
urn:us:gov:ic:aces:ntk:enterprise:role:permissive	Enterprise Role Permissive
urn:us:gov:ic:aces:ntk:enterprise:role:restrictive	Enterprise Role Restrictive
urn:us:gov:ic:aces:ntk:ico	Intelligence Community Only
urn:us:gov:ic:aces:ntk:license	License
urn:us:gov:ic:aces:ntk:mn	Mission Need Profile
urn:us:gov:ic:aces:ntk:nd	No Distribution
urn:us:gov:ic:aces:ntk:oc	Originator Controlled

CVEnumNTKAccessPolicy Values	
Value	Documentation
urn:us:gov:ic:aces:ntk:permissive	Permissive group/individual access
urn:us:gov:ic:aces:ntk:propin:1	PROPIN for US Government Employees
urn:us:gov:ic:aces:ntk:propin:2	Explicit PROPIN
urn:us:gov:ic:aces:ntk:rac	Restricted activities under the authority category
urn:us:gov:ic:aces:ntk:restrictive	Restrictive group access

## Chapter 26 - CVEnumNTKProfileDes for ISM

### 26.1 - Descriptive information

- Description: NTK ProfileDes namespaces identify the type of NTK. All NTK enterprise profile namespace URNs start with 'urn:us:gov:ic:ntk:profile'. Values in this CVE correspond to the terminating portion of NTK profile namespace URNs.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:ntk:profiledes
- Created: 2015-09-04T10:54:00-04:00
- Source: NTK DES
- Point of contact:
  - Office of the IC CIO
  - E-mail: [ic-standards-support@odni.gov](mailto:ic-standards-support@odni.gov)

### 26.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumNTKProfileDes.xml

**Table 27 - CVEnumNTKProfileDes Values**

CVEnumNTKProfileDes Values	
Value	Documentation
urn:us:gov:ic:ntk:profile:agencydissem	Agency Dissem
urn:us:gov:ic:ntk:profile:datasphere	Data Sphere
urn:us:gov:ic:ntk:profile:group-ind	Group and Individual
urn:us:gov:ic:ntk:profile:role	ROLE