Spatial Data Standards for Facilities, Infrastructure, and Environment (SDSFIE)

SDSFIE Metadata (SDSFIE-M): Implementation Guidance

Version 1.0
(8 SEP 2015)

Prepared By:
The IGI&S Governance Group (IGG) for
The Assistant Secretary of Defense (Energy, Installations & Environment)
© 2015
Executive Summary

This document contains implementation guidance for the Spatial Data Standards for Facilities, Infrastructure, and Environment (SDSFIE) - Metadata standard, or SDSFIE-M. SDSFIE-M is a community standard for geospatial metadata, registered in the DoD IT Standards Registry (DISR). SDSFIE-M is a profile of the National System for Geospatial-Intelligence (NSG) Metadata Foundation, or NMF. NMF is, in turn, a profile of ISO 19115:2003/Cor 1:2006 (Geographic Information – Metadata).

SDSFIE-M is applicable to (and mandated for use by) the Installation Geospatial Information and Services (IGI&S) user community, as defined in DoD Instruction (DoDI) 8130.01. This standard is intended to describe IGI&S spatial data holdings and services (e.g. those structured according to the Spatial Data Standard for Facilities, Infrastructure, and Environment-Vector (SDSFIE-V)).

This document defines the general requirement for IGI&S metadata and expresses, as a series of rules, other implementation requirements for SDSFIE-M such as the need for metadata to be accessible, the requirement to establish milestones and deadlines for the implementation of SDSFIE-M mandated versions, and the need for Components to develop their own implementation plans.

Information security is a very important topic with respect to metadata and this document provides rules concerning how information security markings shall be expressed for both metadata and the resources that the metadata describes.

Geospatial metadata is best created and maintained via automated tools. This document includes a rule that any tool that is developed by an IGG member organization must conform to the rules defined in this guidance.
Revision History

<table>
<thead>
<tr>
<th>Description</th>
<th>Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial IGG Approved Version</td>
<td>8 SEP 2015</td>
<td>1.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

Executive Summary ............................................................................................................. 2  
1 Overview .......................................................................................................................... 6  
2 Requirement for IGI&S Metadata ..................................................................................... 6  
3 Rules for Implementing SDSFIE-M ................................................................................. 7  
4 Metadata and Resource Constraint Rules ..................................................................... 10  
   4.1 Overview .................................................................................................................... 10  
   4.2 Legal Constraints ....................................................................................................... 10  
   4.3 Security Constraints ................................................................................................. 11  
      Classification .............................................................................................................. 11  
      Classification System ............................................................................................... 11  
      User Note .................................................................................................................... 12  
   Handling Description .................................................................................................... 12  
   Owner / Producer .......................................................................................................... 12  
   Dissemination Controls ............................................................................................... 12  
   Atomic Energy Act Information .................................................................................... 14  
   Foreign Government Information (FGI) ..................................................................... 15  
   Distribution Statements ............................................................................................... 16  
5 Metadata Tools .............................................................................................................. 18  
   5.1 SDSFIE-M Metadata Style for ArcGIS ................................................................... 18  
6 References ....................................................................................................................... 18  
7 Definitions ....................................................................................................................... 19  
8 Abbreviations ............................................................................................................... 19  
9 Versioning Lifecycle States .......................................................................................... 20
1 Overview

This document contains implementation guidance for the Spatial Data Standards for Facilities, Infrastructure, and Environment (SDSFIE) - Metadata standard, or SDSFIE-M. SDSFIE-M is a community standard for geospatial metadata, registered in the DoD IT Standards Registry (DISR). SDSFIE-M is a profile of the National System for Geospatial-Intelligence (NSG) Metadata Foundation, or NMF. NMF is, in turn, a profile of ISO 19115:2003/Cor 1:2006 (Geographic Information – Metadata).

SDSFIE-M is applicable to (and mandated for use by) the Installation Geospatial Information and Services (IGI&S) user community, as defined in DoD Instruction (DoDI) 8130.01. This standard is intended to describe IGI&S spatial data holdings and services (e.g. those structured according to the Spatial Data Standard for Facilities, Infrastructure, and Environment-Vector (SDSFIE-V)).

Geospatial data can take many forms, making rapid search and discovery difficult. This is the reason why DoD developed the SDSFIE-M standard. The structure of SDSFIE-M supports the goals of making IGI&S data discoverable by automated means, understandable to users, and thus more trusted for DoD missions and decision making. By making IGI&S data discoverable, understandable, and trusted we provide users and managers the data awareness they need to prevent duplication of data acquisition. This allows DoD to focus scarce resources on acquiring only that data which is truly needed, and focuses data maintenance effort where it will provide the most cost-effective benefit to the enterprise.

2 Requirement for IGI&S Metadata

In accordance with DoDI 8320.02 and as implemented by DoDI 8130.01 (with respect to IGI&S), all DoD IT resources shall be made discoverable, understandable, and trusted to the extent allowed by law and policy. These policies also support the goals of several federal executive orders, including EO 12906 (as implemented by OMB Circular A-16) and a host of transparency and open government issuances (summarized in OMB Memorandum M-13-13, “Open Data Policy—Managing Information as an Asset”). DoDI 8320.02 furthermore establishes the requirement that all DoD activities implement the applicable standards cited in the DoD IT Standards Registry (DISR), and that all authoritative data sources (ADSs) must be registered in the DoD Data Services Environment (DSE). A key element of DSE registration is the filing of a DoD Metadata Search (DDMS) record, which is a subset of the elements contained in an SDSFIE-M record.

Taken together these policies establish the mandate that DoD organizations which create or maintain IGI&S must conform to the SDSFIE standards that are registered in the DISR, including the SDSFIE-V and SDSFIE-M standards. SDSFIE-M records must be created for each applicable SDSFIE-compliant data set or geospatial service within DoD, and these records must be made discoverable within the Joint Information Enterprise as directed by the policy statements contained in DoDI 8130.01. SDSFIE-M records may also be created for other IGI&S data sets or services, at the discretion of the authoring organization.

To maintain interoperability and to establish a coordinated approach to IGI&S, each DoD Component shall follow the common guidance contained in this document to implement SDSFIE-M. The key elements of this guidance include:

- General rules that govern the implementation of SDSFIE-M (section 3).
• Rules and guidance pertaining specifically to metadata and resource constraints (section 4).
• Implementing guidance pertaining to automated metadata tools, specifically the SDSFIE-M Metadata Style for ArcGIS (section 5).
• Metadata implementation references (section 6).

3 Rules for Implementing SDSFIE-M

The IGI&S Governance Group (IGG) shall govern the implementation of SDSFIE-M in accordance with these rules:

Rule 3-1 Applicability

1) All DoD organizations subject to IGI&S standards (as defined in DoDI 8130.01) and that implement SDSFIE-M must conform to this implementation guidance.

2) This document (and its revisions) applies to all Mandated or Emerging versions of SDSFIE-M. It also applies to all Retired SDSFIE-M versions. See section 9 for the definition of Emerging, Mandated, and Retired.

Rule 3-2 SDSFIE-M Versioning¹

1) SDSFIE-M shall employ a three-level version pattern where major, minor, and corrigendum versions are specified using integers, separated by periods (for example, 1.0.2). Until a corrigendum release exists, a two-level version pattern (for example, 1.1) will be used in practice.

2) Revisions of SDSFIE-M are defined as follows:
   a. A major revision re-structures metadata elements in such a way that would significantly change the organization of existing implementation files. This type of change might occur when revising SDSFIE-M to conform to a new ISO metadata standard. The initial version of a major revision has minor (and corrigendum) version set to zero.
   b. A minor revision is one where the changes do not significantly change the organization of existing implementation files. This type of change might occur when new capability is added to SDSFIE-M through the introduction of one or more new elements. For example, extending the MD.FeatureCatalogue element to include attribute, enumeration, and enumerant information will likely require a new minor revision. The version attribute shall use the Major.Minor version number initially set at 0 and shall be incremented after each minor version (e.g., 4.0 to 4.1).
   c. A corrigendum, defined as a “bug-fix”, is used to correct errors in previous versions with the same Major.Minor version designation. The version attribute shall use the

complete Major.Minor.Corrigendum version number initially set at 0 and shall be incremented after each bug fix (e.g., 4.0 to 4.0.1 or 4.1.2 to 4.1.3).\(^2\)

3) Only major and minor revisions will be considered as triggers for changing the specification’s status in the DISR.

4) The IGG shall determine when to recommend changing the lifecycle status of a version to Emerging or Mandated.

**Rule 3-3  Mandated SDSFIE-M Version Milestones**

1) As a condition of mandating an SDSFIE-M version, milestones and deadlines for the implementation of the standard shall be developed by the IGG. The IGG will forward these recommended milestones and deadlines to the ASD(EI&E) in accordance with DoDI 8130.01. The following milestones (each of which should have a deadline) are necessary, as a minimum:

   a) Completion (including IGG acceptance) of an implementation specification or SMIS.

   b) Development of implementation tools such as an ArcGIS Metadata Style, or equivalent.

   c) Completion of Component implementation plans as defined in rule 3-4.

   d) Milestone(s) for when all Components shall have complete metadata records for all applicable IGI&S data or services; this may be a sequence of milestones (e.g. percent completion goals) and may vary based on the type of data (i.e. vector, raster, services).

**Rule 3-4  Component Implementation Plans**

1) Within nine months of a Major version being mandated, or six months of a Minor version, Components shall develop an SDSFIE-M implementation plan aligning to the milestones and deadlines developed under Rule 3-3. Components may use one or more documents, but must include the following content (often referred to as a plan of action and milestones or POAM):

   a) Metadata Development Plan and Schedule

      i) A high-level description of the plan for developing metadata for their undocumented or newly created data holdings.

      ii) A schedule for the metadata development.

   b) Metadata Migration Plan and Schedule

      i) A high-level description of the plan for migrating existing metadata from the current version (or a previous standard) to the new version.

      ii) A schedule for the metadata migration.

---

\(^2\) This versioning scheme is widely used for GEOINT standards and is specified in “Policy Directives for Writing and Publishing OGC Standards, Section 13, Document 06-135r7, Open Geospatial Consortium, 15 June, 2009.
2) Components shall submit their implementation plans to the IGG Chair, who will review and validate that the plans conform to this implementation guidance. Initial review comments or validation will be returned within 30 days of submission.

3) After first informing the Component and allowing not less than two weeks for their response, the IGG Chair shall inform the IGG of the results of this review in a timely manner.

4) Components may formally request an exception to the required milestones and deadlines to the IGG Chair, who shall follow the consensus process defined in the SDSFIE Governance Plan.

**Rule 3-5 Existence of Metadata**

1) All IGI&S data holdings shall be documented with SDSFIE-M compliant (the current DISR Mandated version) metadata unless the data is classified.
   a) This requirement is intended to apply to all vector and raster data produced directly by or for the Components, as well as geospatial services provided by them.
   b) This requirement is not intended to apply to data created for one-time, project-specific requirements (for example, those not standardized by SDSFIE).

2) Classified IGI&S data holdings shall be documented using NSG Metadata Foundation (NMF) compliant metadata (the current DISR Mandated version).

3) Metadata is required at the entity (feature or object type) level only.
   a) This requirement is not intended to apply to feature level metadata.

**Rule 3-6 Accessibility of Metadata; Support to Discovery**

1) Components shall make metadata records accessible to the DoD IGI&S enterprise via the Defense Installations Spatial Data Infrastructure (DISDI) Program either statically or dynamically.

2) If the Component provides records statically, they shall be delivered annually as valid SDSFIE-M XML (SMIS) documents to the DISDI Program for cataloging on the DISDI Portal.

3) If the Component provided records dynamically, they shall be maintained in an enterprise-accessible catalog that is registered with and searchable from the DISDI Portal by federation or other technique.

**Rule 3-7 Component-level Governance**

---

3 XML validation is the process of checking a document written in XML (eXtensible Markup Language) to confirm that it is both well-formed and also “valid” in that it follows a defined structure. A well-formed document follows the basic syntactic rules of XML, which are the same for all XML documents. Valid means that the XML document follows the structure of SMIS schema hosted at http://metadata.ces.mil/dse/ns/DISDI/smis/version, where version is the currently mandated version of the SMIS. This structural validation is determined using a validating parser or validation tool to read the document and compare it against the schema.
1) Component-level governance is the responsibility of the Component's IGI&S Program Manager.

2) A key element of the Component-level governance is the existence of written implementation guidance (may be part of the Component’s SDSFIE-M implementation plan or other guidance) which has been reviewed and validated by the IGG Chair.

Rule 3-8 SMIS Document Content
1) SDSFIE-M XML (SMIS) documents shall include all mandatory and applicable conditional elements.

4 Metadata and Resource Constraint Rules

This section contains an explanation of and rules for the marking of metadata and resources with information about legal and security constraints. The security constraints apply only to UNCLASSIFIED data (see Rule 3-5.2). Additionally, the constraints are NOT intended to support an automated access determination.

4.1 Overview

To document access and use requirements in SDSFIE-M, constraint information is used to describe the legal and security constraints placed on the resource as well as on the metadata itself. In other words, SDSFIE-M requires at least two constraints on the metadata and at least two constraints on the resource (one each for legal and security constraints). These must be included even if the constraint states that there is no actual constraint.

4.2 Legal Constraints

The legal constraint elements contain restrictions and legal prerequisites for access and use of the resource or metadata. Access constraints and use constraints are both drawn from a code list that details the type of restriction on access and use, respectively. The restriction types are copyright, license, US Privacy Act, intellectual property, simply restricted (e.g., for legal reasons), other restrictions, or no restriction. Also included in the security constraints are use limitations that are textual description of the legal constraint.

Rule 4-1 Legal Constraints on Metadata and Resource
1) Legal constraints on both the metadata and the resource shall be documented using legal constraint elements.

---

4 While an eventual goal is to enable the automated access decision, it is just too early in the lifecycle of SDSFIE-M and its implementation to expect that these kind of decisions can be fully automated. Nevertheless, SDSFIE-M utilizes the same specifications that are implemented in other parts of DoD and the Intelligence Community so that our community is in alignment with the standards governing information systems marking and need-to-know. In the future, SDSFIE-M may likely be based on the XML Data Encoding Specification for Access Rights and Handling (ARH.XML) which encapsulates both ISM.XML and NTK.XML.

5 The legal rules are based on the metadata elements defined in the MD_LegalConstraints model from ISO 19115.
2) If there are no legal constraints on either the metadata or the resource, then the elements shall indicate the lack of a constraint.

### 4.3 Security Constraints

The security constraint elements contain handling restrictions imposed on the resource or metadata for national security or other concerns.

#### Classification

There are only three classification levels defined in EO 13526: “CONFIDENTIAL”, “SECRET”, and “TOP SECRET”. “UNCLASSIFIED” is a marking (not a classification level) that indicates the information does not meet the threshold for classification as defined in EO 13526. As stated in Rule 3-5.2, classified metadata and resources are documented using NMF and are outside the scope of this section.

**Rule 4-2 Classification of Metadata and Resource**

1) The marking of SDSFIE-M metadata and resources shall be “UNCLASSIFIED” (per rule 3-5).

2) If the metadata or resource has multiple owner/producers, then the marking of SDSFIE-M metadata and resources shall be “JOINT UNCLASSIFIED [LIST]”. Where “[LIST]” pertains to a list of trigraph/tetragraph codes representing the owner/producer country[ies] or organization[s].

3) A “JOINT” marking, must be accompanied by an “AUTHORIZED FOR RELEASE TO [USA, LIST]” or “REL TO [USA, LIST]” marking. Where “[USA, LIST]” pertains to the string that contains “USA” followed by a list of trigraph/tetragraph codes representing country[ies] or organization[s] that are approved to receive a release.

4) If the metadata or resource has an owner/producer of NATO or an “ATOMAL” marking, then the marking of SDSFIE-M metadata and resources shall be “NATO UNCLASSIFIED”.

#### Classification System

The classification system being used is the Intelligence Community Markings System, formerly known as US CAPCO. Despite this fact, the current version of NMF and SDSFIE-M both require a reference to US CAPCO.

**Rule 4-3 Classification System**

The classification system for SDSFIE-M shall be “US CAPCO”.

---

6 The security rules are based on the metadata elements defined in the MD_SecurityConstraints model from ISO 19115 and extended by the National System for Geospatial-Intelligence Metadata Foundation (NMF) NMF_SecurityContraints model. The NMF_SecurityContraints integrates the Intelligence Community Technical Specifications, XML Data Encoding Specification for Information Security Markings (ISM.XML) and XML Data Encoding Specification for Need-To-Know Metadata (NTK.XML). They are also based on the content of the Intelligence Community Markings System, Register and Manual (IC Markings, formerly the CAPCO Manual).
User Note
A user note is optional and contains an explanation of the application of the legal constraints or other restrictions and legal prerequisites for obtaining and using the resource or metadata.

Handling Description
A handling description is optional and provides additional information about the restrictions on handling the resource or metadata.

Owner / Producer
The national government(s) or international organization(s) that have purview over the classification marking of an information resource or portion therein are the owner/producer(s).

Rule 4-4 Owner/Producer

1) At least one owner/producer shall be indicated for the metadata and for the resource.

2) If more than one owner/producer is indicated, then the metadata or resource shall be given the classification “JOINT UNCLASSIFIED [LIST]”. Where “[LIST]” pertains to a list of trigraph/tetragraph codes representing the owner/producer country[ies] or organization[s].

3) If more than one owner/producer is indicated and one of the owner/producers is NATO or the sole owner/producer is NATO, then the metadata or resource shall be given the classification “NATO UNCLASSIFIED”.

4) The owner/producer of the metadata and the resource need not be the same, although release decisions for jointly owned metadata or resources must be agreed and documented in an “AUTHORIZED FOR RELEASE TO [USA, LIST]” or “REL TO [USA, LIST]” marking. Where “[USA, LIST]” pertains to the string that contains “USA” followed by a list of trigraph/tetragraph codes representing country[ies] or organization[s] that are approved to receive a release.

Dissemination Controls
Dissemination Controls are control markings that identify the expansion or limitation on the distribution of information. These markings are in addition to and separate from the levels of classification defined by EO 13526. The metadata or the resource can have a Dissemination Control. Typically, the resource dissemination control will be more stringent than the metadata.

The Dissemination Control markings possible in SDSFIE-M are divided into three groups, IC, non-IC, and other. Table 1 contains the allowable Dissemination Control markings along with their definition and Foreign Disclosure and Release (FD&R) possibility and is provided to guide users in selecting appropriate Dissemination Control markings.

Table 1: Dissemination Control Markings Allowed in SDSFIE-M with FD&R Possibility

<table>
<thead>
<tr>
<th>Title</th>
<th>Abbreviation</th>
<th>Definition</th>
<th>FD&amp;R Possible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence Community (IC) Dissemination Control Markings</td>
<td>FOR OFFICIAL USE ONLY</td>
<td>FOUO</td>
<td>Intelligence marking used for UNCLASSIFIED official government information that is withheld from public release until approved for release by the originator.</td>
</tr>
<tr>
<td>CAUTION- PROPRIETARY INFORMATION INVOLVED</td>
<td>PROPIN</td>
<td>Marking used to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This marking may be used on government proprietary information only when the government proprietary information can provide a contractor(s) an unfair advantage, such as US Government budget or financial information.</td>
<td>YES</td>
</tr>
<tr>
<td>DEA SENSITIVE</td>
<td>DSEN</td>
<td>Unclassified information originated by DEA that requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.</td>
<td>YES</td>
</tr>
<tr>
<td>FOREIGN INTELLIGENCE SURVEILLANCE ACT</td>
<td>FISA</td>
<td>The Foreign Intelligence Surveillance Act (FISA) of 1978, as amended, prescribes procedures for the physical and electronic surveillance and collection of &quot;foreign intelligence information&quot; between or among &quot;foreign powers&quot; on territory under United States control. The marking denotes the presence of FISA material.</td>
<td>NO</td>
</tr>
<tr>
<td>NOT RELEASABLE TO FOREIGN NATIONALS</td>
<td>NOFORN</td>
<td>NOFORN is an explicit foreign release marking used to indicate the information may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens without permission of the originator and in accordance with provisions of DCID 6/7, ICD 403, NDP-1, and implementation guidance in IC Markings.</td>
<td>NO</td>
</tr>
</tbody>
</table>

**Non-Intelligence Community (non-IC) Dissemination Control Markings**

| LIMITED DISTRIBUTION | LIMDIS | Marking used to identify unclassified maps, geospatial products and data sets, which the Secretary of Defense may withhold from public release. Release or disclosure of these products is limited to Department of Defense (DOD) and DOD contractors (including any sub-contractors), and, for national intelligence purposes, to the Director of National Intelligence (DNI), non-DOD members of the Intelligence Community (IC), and the National Security Council (NSC), and, with permission from NGA, to other Federal Government departments and agencies. Contact NGA Disclosure and Release for further guidance at: NDRO@Nga.Ic.Gov (Intelink-TS), NDRO@NGA.Smil.Mil (Intelink-S), or NDRO@NGA.Mil. | YES |
| EXCLUSIVE DISTRIBUTION | EXDIS | Information with exclusive distribution to officers with essential need-to-know. This caption is used only for highly sensitive traffic between the White House, the Secretary, Deputy, or Under Secretaries of State and Chiefs of Missions. | YES |
| NO DISTRIBUTION | NODIS | This control is used only on messages of the highest sensitivity between the President, the Secretary of State, and Chief of Mission. No further dissemination is allowed to any other than the original addressee(s) without the approval of the Executive Secretary. | NO |
| SENSITIVE BUT UNCLASSIFIED | SBU | Administrative unclassified information originated from within the Department of State, which warrants a degree of protection and administrative control and meets criteria for exemption from mandatory public disclosure under the Freedom of Information Act. | YES |
| SENSITIVE BUT UNCLASSIFIED NOFORN | SBU NOFORN | Administrative unclassified Information originated within the Department of State that warrants a degree of protection and administrative control, meets criteria for exemption from mandatory public disclosure under the Freedom of Information Act, and is prohibited for dissemination to non-US citizens. | NO |
| LAW ENFORCEMENT SENSITIVE | LES | LES information is unclassified information originated by agencies or elements with law enforcement missions that may be used in criminal prosecution and that requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence, or the integrity of pretrial investigative reports. Any law enforcement agency employee or contractor in the course of performing assigned duties may designate information as LES if authorized to do so pursuant to department specific policy and directives. | YES |
LAW ENFORCEMENT SENSITIVE NOFORN | LES NOFORD | LES NOFORD information is unclassified information originated by agencies with law enforcement missions that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence, or the integrity of pretrial investigative reports, and is prohibited from dissemination to foreign nationals. Any law enforcement agency employee or contractor in the course of performing assigned duties may designate information as LES NOFORD if authorized to do so pursuant to department-specific policies and directives. | NO

| PROTECTED CRITICAL INFRASTRUCTURE INFORMATION | PCII | PCII is a category of Sensitive but Unclassified (SBU) information that is afforded protections from (a) disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws and (b) use in civil litigation or for regulatory purposes. The PCII Program is unique because it provides a method for critical infrastructure owners to submit information voluntarily to the Federal government that the government would not otherwise have access to. Once information is submitted and the PCII Program has validated it as PCII, Federal, State, and local government entities can use the information to protect the Nation’s critical infrastructure. PCII is accessed only by authorized users who have a need-to-know specified PCII. | NO

| SAFEGUARDS INFORMATION | SGI | SGI is a special category of sensitive, unclassified information required by Section 147 of the Atomic Energy Act to be protected. | NO

Rule 4-5 Dissemination Control Marking

1) All metadata and resources whose dissemination must be controlled shall use one or more of the Dissemination Control markings listed in Table 1.

2) All metadata and resources shall be marked with the least restrictive applicable Dissemination Control marking(s) possible, subject to the additional guidance found in IC Markings.

3) All metadata and resources with a Dissemination Control shall also include a Distribution Statement this is consistent with the Dissemination Control. For example, it is inconsistent to have a Dissemination Control and use Distribution A.

Rule 4-6 FD&R Marking of Dissemination Controlled Information

1) All metadata and resources marked with any of the Dissemination Control markings listed in Table 1 with an affirmative FD&R possibility shall also be marked as “NOFORN” in the absence of a positive release determination by the originating agency. If a positive release determination is made by the originating agency, then the “NOFORN” marking shall be removed.

2) All metadata and resources marked with any of the Dissemination Control markings listed in Table 1 with a negative FD&R possibility shall also be marked as “NOFORN”.

Atomic Energy Act Information

Atomic Energy Act (AEA) information markings are used in SDSFIE-M to denote the presence of unclassified DoD Unclassified Controlled Nuclear Information (marked “DOD UCNI” or “DCNI”) and DOE Unclassified Controlled Nuclear Information (marked “DOE UCNI” or “UCNI”).

“DOD UCNI” is unclassified information regarding security measures for the physical protection of DoD Special Nuclear Material (SNM), equipment or facilities. Material is designated as “DOD UCNI” only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common
defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion or sabotage of DoD SNM, equipment or facilities.

“DOE UCNI” applies to information that has been declassified or removed from the Restricted Data” (RD) category but may not be disseminated to the general public. Included are certain unclassified aspects of design of the nuclear production and utilization facilities; security measures for production/utilization facilities, nuclear material contained in such facilities, and nuclear material in transit; as well as unclassified design, manufacture, and utilization information of any atomic weapon or component.

Rule 4-7 Atomic Energy Act Information Markings

1) Atomic Energy Act Information shall be marked with either “DOD UNCI” or “DOE UNCI” as appropriate.

2) A “DOD UCNI” or “DOE UCNI” marking requires that the information be handled as “NOFORN” when considering foreign disclosure and release, unless an affirmative decision has been made by the originating agency’s FD&R authority.

Foreign Government Information (FGI)

Under EO 13526, Foreign Government Information is defined as:

- Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

- Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

- Information received and treated as “Foreign Government Information” under the terms of a predecessor order.

Foreign Government Information (“FGI”) markings are used in US products to denote the presence of classified or unclassified foreign owned or produced information, and the foreign source(s), if they may be acknowledged. These markings are used based on sharing agreements or arrangements with the source country or international organization.

Rule 4-8 Foreign Government Information Markings

1) Foreign Government Information shall be marked with:

   a. “FGI [LIST]” ([LIST] pertains to a list of trigraph/tetragraph codes representing the country[ies] or organization[s] of origin), or

   b. “FGI” (when country[ies] or organization[s] of origin must be concealed)

2) If the originating country allows further sharing by the United States, an “AUTHORIZED FOR RELEASE TO [USA, LIST]” or “REL TO [USA, LIST]” marking must be used. Where “[USA, 

---

7 Restricted Data is defined as all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but must not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.
LIST)” pertains to the string that contains “USA” followed by a list of trigraph/tetragraph
codes representing country[ies] or organization[s] that are approved to receive a release.

3) If the originating country prohibits further sharing by the United States, a “NOFORN”
marking shall be used.

**Distribution Statements**

**Rule 4-9 Use of Distribution Statements**

Metadata and resources shall be marked using the distribution statements defined by DoDI 5230.24.

Although DoDI 5230.24 is only mandatory for marking and managing technical documents
(including research, development, engineering, test, sustainment, and logistics information), it is
widely used in the GEOINT community to mark GI&S data and products, a use which is not
prohibited by the policy.

The statements defined in DoDI 5230.24 are used to denote the extent to which they are
available for secondary distribution, release, and dissemination without additional approvals or
authorizations. Table 5 from 5230.24, recreated for convenience below as Table 2, defines a
series of distribution statements that are used to inform approved distribution and the reasons
for those distribution decisions.

**Table 2: Distribution Statements and Their Corresponding Reasons for Use**

<table>
<thead>
<tr>
<th>Distribution A</th>
<th>Approved for public release: distribution unlimited.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution B</td>
<td>Distribution authorized to U.S. Government agencies (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).</td>
</tr>
<tr>
<td>Distribution C</td>
<td>Distribution authorized to U.S. Government agencies and their contractors (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).</td>
</tr>
<tr>
<td>Distribution D</td>
<td>Distribution authorized to Department of Defense and U.S. DoD contractors only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).</td>
</tr>
<tr>
<td>Distribution E</td>
<td>Distribution authorized to DoD Components only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).</td>
</tr>
<tr>
<td>Distribution F</td>
<td>Further dissemination only as directed by (controlling office) (date of determination) or higher DoD authority.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reason</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUBLIC RELEASE.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADMINISTRATIVE OR OPERATIONAL USE: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may apply to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>CONTRACTOR PERFORMANCE EVALUATION: To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRITICAL TECHNOLOGY: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>DIRECT MILITARY SUPPORT: The document contains export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operational military advantage of the United States, another country, or a joint U.S.-foreign program. Designation of such data is made by competent authority in accordance with Reference (d).</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>EXPORT CONTROLLED: To protect information subject to the provisions of Reference (d).</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>FOREIGN GOVERNMENT INFORMATION: To protect and limit distribution in accordance with the desires of and agreements with the foreign government that furnished the technical information.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>OPERATIONS SECURITY: To protect information and technical data that may be observed by adversary intelligence systems and determining what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PREMATURE DISSEMINATION: To protect patentable information on systems or processes in the development or concept stage from premature dissemination.</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PROPRIETARY INFORMATION: To protect information not owned by the U.S. Government and marked with a statement of a legal property right. This information is received with the understanding that it will not be routinely transmitted outside the U.S. Government.</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>TEST AND EVALUATION: To protect results of test and evaluation of commercial products or military hardware when disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SOFTWARE DOCUMENTATION: To protect technical data relating to computer software that is releasable only in accordance with the software license in subpart 227.72 of Reference (s). It includes documentation such as user or owner manuals, installation instructions, operating instructions, and other information that explains the capabilities of or provides instructions for using or maintaining computer software.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SPECIFIC AUTHORITY: To protect information not specifically included in the above reasons, but which requires protection in accordance with valid documented authority (e.g., Executive orders, statutes such as Atomic Energy Federal regulation). When filling in the reason, cite “Specific Authority (identification of valid documented authority).”</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>VULNERABILITY INFORMATION: To protect information and technical data that provides insight into vulnerabilities of U.S. critical infrastructure, including DoD warfighting infrastructure, vital to National Security that are otherwise not publicly available.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
5 Metadata Tools

The DISDI Program and Components may develop and disseminate tools that support the implementation of SDSFIE-M (and metadata generally) across the IGI&S community. This implementation guidance does not make any one tool mandatory for use by all Components primarily because the IGI&S community uses multiple software vendors and different vendors handle metadata differently.

Rule 5-1 Tools Must Conform

Any tool that is developed by any IGG member organization for the implementation of SDSFIE-M shall conform to the rules defined in this guidance.

5.1 SDSFIE-M Metadata Style for ArcGIS

The DISDI Program has developed a metadata style for use with the Esri ArcGIS platform and plans to continue updating it, subject to availability of resources.

A metadata style configures ArcGIS to create metadata according to a particular metadata standard and workflow. Choosing a metadata style is like applying a filter to an item's metadata. The style controls how you view the metadata and also the pages that appear for editing metadata in the Description tab in ArcGIS. The SDSFIE-M Metadata Style for ArcGIS is designed to support SDSFIE Metadata Implementation Schema (SMIS). Therefore, the style will determine how metadata is exported and validated for SDSFIE-M.

6 References

The following referenced documents provide the background for SDSFIE-M and these implementation guidelines.


7 Definitions

This section provides definitions for terms used in this document.

**Component**

A Military Department, Defense Agency, DoD Field Activity, or organization within the Office of the Secretary of Defense

**IGI&S Programs**

The DoD Component headquarters level activities responsible for oversight, policy, and guidance pertaining to installation geospatial information and services.

**Implementation**

The creation and maintenance of metadata for geographic information system data holdings.

**Implementation Compliance**

Compliance is measured with respect to a metadata standard. An Implementation is considered compliant if metadata documents can be generated that validate against the SMIS schema for the currently mandated version of SDSIFE-M.

8 Abbreviations

ASD (Ei&E) – Assistant Secretary of Defense (Energy, Installations & Environment)

CIP – Common Installation Picture

CMP – Change Management Process

COI – Community of Interest

DISDI – Defense Installations Spatial Data Infrastructure

DISR – Department of Defense Information Technology Standards Registry

DoD – Department of Defense

DOE – Department of Energy

DoDI – Department of Defense Instruction

Ei&E – Energy, Installations & Environment

GEOINT – Geospatial Intelligence

IGI&S – Installation Geospatial Information & Services

IGG – IGI&S Governance Group

ISO – International Organization for Standardization
The following set of versioning lifecycle states if taken from the SDSFIE Governance Plan and is repeated here for the convenience of the reader.

1) Emerging
   a) The version is created and approved but it is not yet Mandated. The version is expected to be Mandated within one to two years. Because each case may be unique, implementing organizations should consider the potential compatibility risks and impacts before considering whether to upgrade to an Emerging standard. For example, upgrading to a minor version may involve less risk than to a major version. The version may be implemented, but not in lieu of Mandated version.

2) Mandated
   a) The version is to be implemented and considered essential for interoperability in the IGi&S community. The milestones and deadlines for implementation of the Mandated version shall be developed by the IGG and approved by ASD (EI&E) in accordance with emerging DoD policy (DoDI 8130.AB).

3) Retired

A version that is no longer Mandated because a new version has been Mandated. Continued use of the Retired version may be allowed if the Component is still in the process of migrating to the mandated version. An implementation plan with milestones may be required by the IGG.