



**United States Strategic Command (USSTRATCOM)**

# **Exposure Verification Tracking Sheet Guide**

Version 1.5

27 December 2007

*Prepared by:*

USSTRATCOM J864

## FORWARD

The main purpose of this guide is to document the Exposure Verification Tracking Sheet Process and provide standard guidance on how to use the sheets to track net-centric compliance.

This Guide is a living document and will continue to be updated with best practices and lessons learned as the Department of Defense (DoD) gains experience implementing data sharing. Suggestions on how to improve this guide are always most welcome.

Comments and recommendations for change to this document may be forwarded to:

USSTRATCOM/J864  
901 SAC BLVD STE 2E10  
OFFUTT AFB NE 68113-6800  
Comm: (402) 294-7926 or DSN: (312) 271-7926  
FAX: (402) 232-7624 or DSN: (312) 272-7624  
NIPRNET E-Mail: [david.waite@stratcom.mil](mailto:david.waite@stratcom.mil)  
SIPRNET E-Mail: [david.waite@stratnets.stratcom.smil.mil](mailto:david.waite@stratnets.stratcom.smil.mil)

## REVISION RECORD

DATE	VERSION	DESCRIPTION OF CHANGE
14 Aug 07	1.0	Initial Release for version 2.0 of the Exposure Verification Tracking Sheets
24 Aug 07	1.1	Updated guide for version 2.1 of the Exposure Verification Tracking Sheets; added "NCES Introduction" section
14 Sept 07	1.2	Added hypertext throughout guide; added "Getting Started" section as well as information about PKI certificates; modified for version 2.11 of the Exposure Verification Tracking Sheets
23 Oct 07	1.3	Modified for change to Joint Capability Areas and subsequent version 2.2 of the Exposure Verification Tracking Sheets; updated MDR information due to MDR version update to 6.1
3 Dec 07	1.4	Added links to NCES user guides; Incorporated lessons learned from Phase 3 of the C2 Data Pilot. Updated Web Service example.
27 Dec 07	1.5	Updated to match version 2.3 of the Exposure Verification Tracking Sheets based on JCS modifications; Modified COI information due to the COI Web Page being moved to the MDR

## TABLE OF CONTENTS

<u>Paragraph</u>	<u>Page</u>
<b>1. Purpose.....</b>	<b>4</b>
<b>2. Background .....</b>	<b>4</b>
<b>3. Why Should I Expose My Data or Service? .....</b>	<b>4</b>
<b>4. Net-Centric Enterprise Services (NCES) Introduction .....</b>	<b>5</b>
4.1 Enterprise Catalog.....	7
4.2 Metadata Registry (MDR) .....	7
4.3 NCES Service Registry .....	7
4.4 Content Discovery and Delivery .....	8
4.5 Federated Search Service.....	8
<b>5. Are You Exposing Data or a Service? .....</b>	<b>8</b>
5.1 Data .....	9
5.2 Services .....	9
5.3 Both Data and a Service .....	10
<b>6. Getting Started .....</b>	<b>12</b>
6.1 DoD PKI Certificates.....	12
6.1.1 Obtaining DoD PKI Software Certificates .....	13
6.1.2 Obtaining ECA/IECA Certificates.....	13
<b>7. How to Fill Out the Exposure Verification Tracking Sheet.....</b>	<b>14</b>
7.1. Data .....	14
7.1.1. Data Visible (Federated Search) Criteria.....	15
7.1.2. Data Accessible (User) Criteria .....	16
7.1.3. Data Understandable Criteria.....	17
7.2. Service.....	18
7.2.1. Service Visible (Registered and Discoverable) Criteria .....	20
7.2.2. Service Accessible (Developer Access) Criteria .....	20
7.2.3. Service Understandable Criteria.....	22
7.3. Examples.....	23
7.3.1. Data.....	23
7.3.2. Service .....	26
<b>8. How to Verify Exposure Verification Tracking Sheet Compliance .....</b>	<b>29</b>
8.1 Verification.....	29
8.2 Lessons Learned.....	30
<b>9. Warning on Foreign Nationals Use of the DISA Metadata Registry (MDR).....</b>	<b>31</b>

[ENCLOSURE A - Glossary](#)

[ENCLOSURE B - References](#)

[ENCLOSURE C - Exposure Status Criteria](#)

[ENCLOSURE D - Exposure Quick Look Checklist](#)

[Figure 1 – Enterprise Services](#)

[Figure 2 – Service, Data & Content Registration](#)

[Figure 3 – Exposure Verification Tracking Sheet Decision Flowchart](#)

[Figure 4 – Data Exposure Verification Tracking Sheet](#)

[Figure 5 – Service Exposure Verification Tracking Sheet](#)

## 1. Purpose

The DoD is moving towards a Net-Centric environment. Part of this effort requires that data and services be exposed so that they are readily available and consumed by the user. The purpose of this guide is to explain the process by which the Exposure Verification Tracking Sheets are used to measure net-centricity in support of the DoD's Net-Centric Data Strategy.

## 2. Background

In October 2006, United States Strategic Command (USSTRATCOM) and United States Joint Forces Command (USJFCOM) partnered, founded, and initiated the C2 Data Pilot. The overarching goal of the C2 Data Pilot is to accelerate the Department of Defense into a net-centric environment by aiding in transitioning global information assets from current stove-piped, point-to-point systems to a service-oriented architecture as directed in [DoD Directive \(DoDD\) 8320.02, "Data Sharing in a Net-Centric Department of Defense."](#) The commands accepted risk by leveraging funds previously identified for near-term capability development in order to realize the long-term benefits of a net-centric environment. While assessing the net-centric status of the Programs of Record, the conclusion was made that a more robust and documented metrics process needed to be put in place. The result of this effort was originally referred to as the "Blue Sheets". The name "Blue Sheets" referred to the background color of the slide that was originally used. These tracking sheets are now referred to as Data and Service Exposure Verification Tracking Sheets.

## 3. Why Should I Expose My Data or Service?

The DoD's vision to establish a Net-Centric Environment is the key to helping the user efficiently and effectively do their job and to ensure they have the tools needed to complete the mission. From the DoD Net-Centric Services Strategy, "When this vision is achieved, all members of the DoD will realize significant benefits. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. Interoperability of capabilities is improved when Military Services, Agencies, and mission partners create reusable "building blocks" through the use of services." <sup>13</sup>

There are three primary components to exposing data and services, Visibility, Accessibility, and Understandability and their definition varies based on whether you are exposing data or a service.

### Visibility

#### *Data*

"Data assets shall be made visible by creating and associating metadata ("tagging"), including discovery metadata, for each asset. Discovery metadata shall conform to the Department of Defense Discovery Metadata Specification. DoD metadata standards shall comply with applicable national and international consensus standards for metadata exchange whenever possible. All metadata shall be discoverable, searchable, and retrievable using DoD-wide capabilities." <sup>4</sup>

### *Services*

"Providers of services must register their services in the enterprise service registry (i.e., publish the metadata describing their services) to ensure that potential users will be able to discover the service. The enterprise-wide service registry will enable all users in the enterprise to find and understand what services already exist, thus facilitating reuse and avoiding investment in the creation of new capabilities." <sup>13</sup>

## **Accessibility**

### *Data*

"Data assets shall be made accessible by making data available in shared spaces. All data assets shall be accessible to all users in the Department of Defense except where limited by law, policy, or security classification. Data that is accessible to all users in the Department of Defense shall conform to DoD-specified data publication methods that are consistent with GIG enterprise and user technologies." <sup>4</sup>

### *Services*

"Users must not only have the ability to discover services, but must also be able to access them in a timely, secure, and effective manner. Service accessibility is controlled by security mechanisms that determine access roles and rules. Decisions on service accessibility are made and implemented by the organizations providing the service based on a variety of factors." <sup>13</sup>

## **Understandability**

### *Data*

"Data assets shall be made understandable by publishing associated semantic and structural metadata in a federated DoD metadata registry." <sup>4</sup>

### *Services*

"Providers of services must use a common set of service description information to enable consistent discovery by users throughout the enterprise." <sup>13</sup>

## **4. Net-Centric Enterprise Services (NCES) Introduction**

NCES is an enabler for information sharing within the DoD as well as with federal, allied, coalition, and multinational partners. These services will be key to making data visible, accessible, and understandable.

NCES will allow users and information systems to:

- Find and access relevant information;
- Expose the information they produce for others to discover;
- Collaborate in a more effective manner;
- Distribute data to forward deployed areas;
- Increase performance and reliability of data access, and;
- Utilize the enterprise infrastructure for evolving DoD systems to a Service-Oriented Architecture.

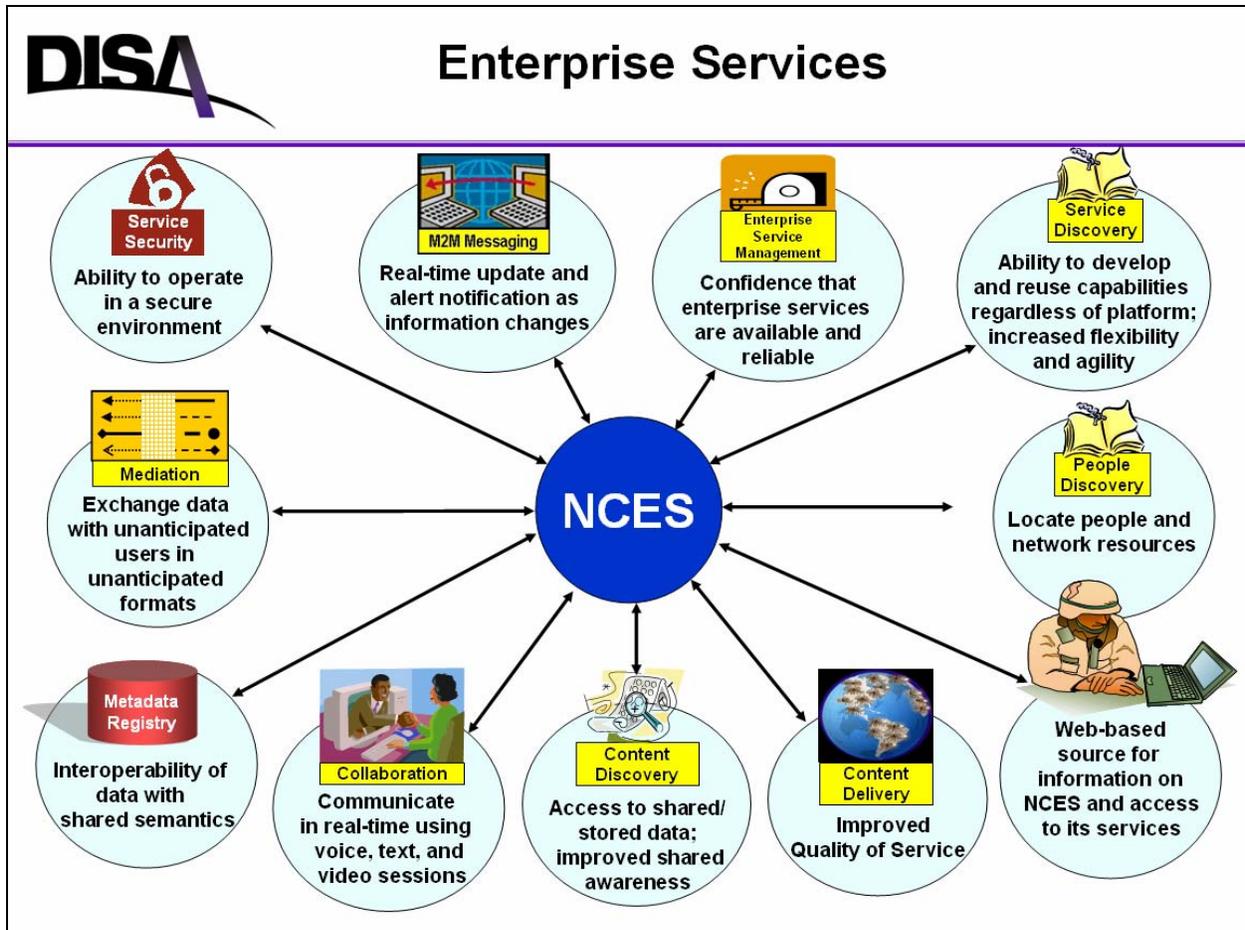


Figure 1 – Enterprise Services

The [Department of Defense Discovery Metadata Specification \(DDMS\)](#) defines discovery metadata elements for resources posted to the community and organizational shared spaces. The purpose of the [DDMS](#) is to provide a uniform set of metadata to describe data assets across the DoD. This enables:

- A finite set of elements to facilitate discovery;
- A clear set of semantics on which discovery is based;
- End users to have confidence in DoD provided search capabilities.

The [Enterprise Catalog](#), the [Metadata Registry](#), and the [NCES Service Registry](#) all use either directly or indirectly the [DDMS](#) element set.

#### **4.1 Enterprise Catalog**

The Content Discovery Core Enterprise Service (CES) is composed of two interface specifications, one of which defines the Enterprise Catalog Service. The Enterprise Catalog Service provides the capability to publish, update, and delete metadata about content for later retrieval via the Federated Search Service. The Enterprise Catalog Service provides the ability for data providers to associate metadata with their content, and to store the metadata in an enterprise-scalable index that is searchable via the Federated Search Specification. The metadata may subsequently be updated or removed by an authorized user. The purpose of the Enterprise Catalog Service is to allow disadvantaged users the ability to "post" content to the enterprise by placing the content onto a network storage location and then publishing the metadata, along with a reference to the content location, to the Enterprise Catalog.

#### **4.2 Metadata Registry (MDR)**

The DoD [MDR](#) enables you to publish metadata artifacts (e.g., schemas, stylesheets, and taxonomies) to a portal available to the DoD community. Making user metadata products visible to the community enables others to reuse the user's hard work and promotes interoperability between systems. To use the services provided, the user must be a registered user on the [MDR Portal](#).

Metadata products are registered in the [MDR](#) by creating a submission package and submitting the package file. Details on building a submission package, using package creation tools, validating the package, and submitting a package are available at (NIPRNet) [https://metadata.dod.mil/mdr/downloads/help/FAQ\\_PackageSubmission.doc](https://metadata.dod.mil/mdr/downloads/help/FAQ_PackageSubmission.doc) or (SIPRNet) [https://metadata.dod.smil.mil/mdr/downloads/help/FAQ\\_PackageSubmission.doc](https://metadata.dod.smil.mil/mdr/downloads/help/FAQ_PackageSubmission.doc). Registered users of the Metadata Registry can access the DoD [MDR Portal](#) at <https://metadata.dod.mil>. The DoD [MDR](#) also provides services access to locate XSL translations between XML schemas at runtime.

#### **4.3 NCES Service Registry**

The [NCES Service Registry](#) provides enterprise-wide insight, control and leverage of an organization's Service Offers assets. Fully supporting the Universal Description, Discovery and Integration ([UDDI](#)) registry standard, the [NCES Service Registry](#) captures Service Offer descriptions and makes them discoverable from a centrally managed, reliable, and searchable location. The [NCES Service Registry](#) is the system of record for Service Offers, providing a foundation for the governance and lifecycle management of these valuable assets.

This user interface provides developers, architects, and business users with the ability to search, browse, and manage the contents of the Registry; publish new artifacts into the Registry; and receive notifications of updates to the Registry. The [NCES Service Registry](#) provides a

configurable user interface, permitting users to work with the Registry at an appropriate level of technical depth.

#### **4.4 Content Discovery and Delivery**

Content Discovery and Delivery is used to query existing data sources, such as databases, catalogs, and search engines, to quickly find stored information. As a data provider, you can use the Enterprise Catalog service to publish metadata about a data source, and the metadata can then be searched using the Content Discovery Federated Search Portlet. If a user wants to access your data, the data will be retrieved and delivered using Content Delivery. The Enterprise Catalog service can be accessed using the service client distributed with the NCES Content Discovery SDK. Alternatively, you may directly implement the Federated Search Web Service and integrate directly with the NCES Content Discovery service.

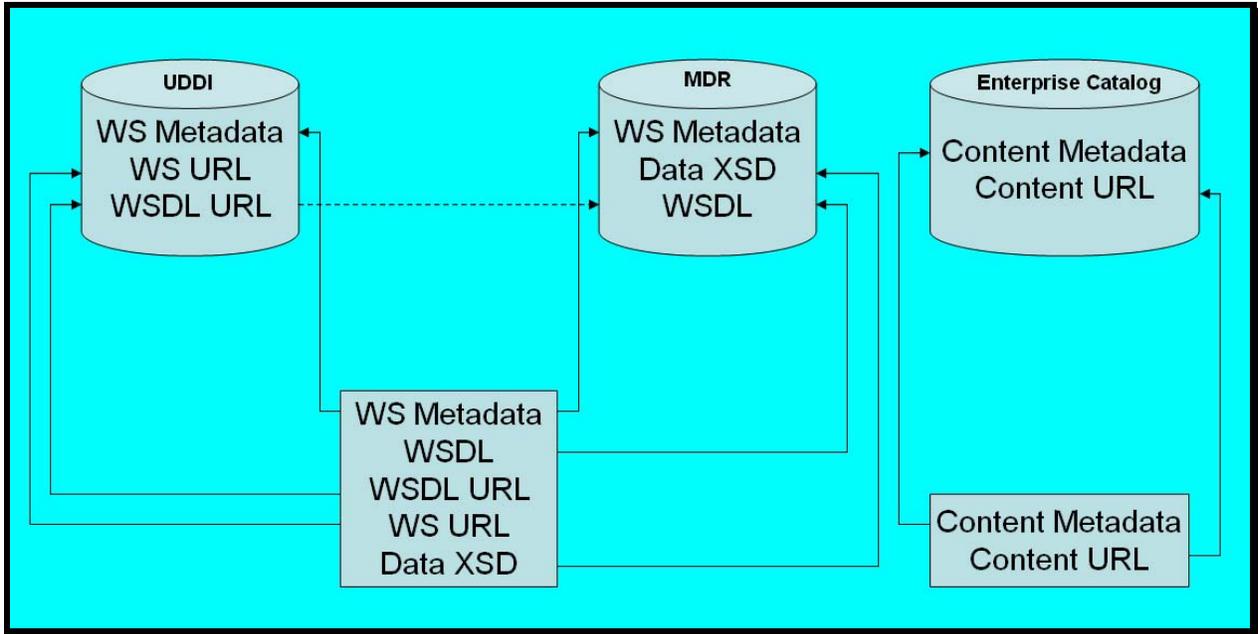
#### **4.5 Federated Search Service**

The Content Discovery CES is composed of two interface specifications, one of which defines the Federated Search Service. The Federated Search Service provides a standard specification for the discovery of metadata from any network attached data source within DOD. The Federated Search Service provides a standard search interface allowing user queries to be brokered to one or more data sources that comply with the Federated Search Specification. The data sources may search the content of Web sites, shared file systems, Structured Query Language (SQL) databases, or existing applications. By encapsulating proprietary interfaces with the Federated Search Specification, legacy Government Off-The-Shelf (GOTS) or Commercial Off-The-Shelf (COTS) data sources can easily expose their metadata to external communities. The Federated Search specification provides for a set of standard metadata using the DOD Discovery Metadata Specification. The use of a standard specification and consistent metadata allows users to leverage multiple data sources using a single application rather than developing multiple point-to-point integrations for each data source.

### **5. Are You Exposing Data or a Service?**

When using the Exposure Verification Tracking Sheets, the first thing that needs to be determined is whether you are exposing data or a service. While on the surface this seems to be a very simple question, experience has shown this can be a very confusing point. The paragraphs below can help demystify this question.

Figure one describes the connections between the Universal Description, Discovery and Integration ([UDDI](#)), Metadata Registry ([MDR](#)), and Enterprise Catalog.



**Figure 2 – Service, Data & Content Registration**

## 5.1 Data

DoDD 8320.02 defines data as, "A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Data and information are equivalent terms for the purposes of this policy."<sup>4</sup>

If you are not using a service ([Web Service](#), Really Simple Syndication ([RSS](#)), Keyhole Markup Language ([KML](#)), Geographically Encoded Objects for RSS Feeds ([GeoRSS](#)), etc...) but rather exposing data directly to the user then you are exposing data and will report using the "Data" template. You will never use the "Service" template for a web page since a web service is machine-to-machine communications and is not a direct user interface function.

## 5.2 Services

Services are constantly evolving for the Internet. As such, measuring net-centricity for these services will need to adjust accordingly when new standards arise. Currently the Exposure Verification Tracking Sheets are designed to be used with [Web Services](#), [RSS](#), [KML](#), and [GeoRSS](#) types of services.

### Web Services

A web service is defined by the [World Wide Web Consortium \(W3C\)](#) as a software system designed to support interoperable Machine to Machine interaction over a network. Web services are frequently just Web APIs that can be accessed over a network, such as the Internet, and executed on a remote system hosting the requested services. The [W3C](#) Web Service definition refers to clients and servers that communicate using Extensible Markup Language (XML) messages that follow the SOAP standard.

## **RSS**

RSS is a family of web feed formats used to publish frequently updated content such as blog entries, news headlines or podcasts. An RSS document, which is called a "feed", "web feed", or "channel", contains either a summary of content from an associated web site or the full text. RSS makes it possible for people to keep up with their favorite web sites in an automated manner that's easier than checking them manually.

## **KML**

KML is an XML-based language for managing the display of three-dimensional geospatial data in application programs. The KML file specifies a set of features (placemarks, images, polygons, 3D models, textual descriptions, etc.) for display in Google Earth, Maps and Mobile. Each place always has a longitude and latitude. Other data can make the view more specific, such as tilt, heading, altitude, which together define a "camera view".

## **GeoRSS**

GeoRSS is an emerging standard for encoding location as part of a RSS feed. RSS is an XML format used to describe feeds ("channels") of content, such as news articles, MP3 play lists, and blog entries. The RSS feeds are rendered by programs such as aggregators and web browsers. In GeoRSS, location content consists of geographical point, lines, or polygons of interest and related feature descriptions. GeoRSS feeds are designed to be consumed by geographic software such as map generators. By building these encodings on a common information model, the GeoRSS collaboration hopes to promote interoperability and "upwards-compatibility" across encodings.

If you are exposing data for machine-to-machine consumption by creating services defined by a "Web Service Description Language (WSDL)", then you are exposing a service and will report net-centric compliance using the "Services" template.

### **5.3 Both Data and a Service**

If your web pages are themselves consuming your own machine-to-machine services (although desired end-state, not currently a general practice), then you are exposing both a service and data and will report the service using the "Services" template and the web page using the "Data" template. Each will be reported independent of the other and will not have a dependency on one another - as the service may be complete and consumable by an unanticipated user; while the web page application may not yet be operational. Use the guidance above for each.

## Exposure Verification Tracking Sheet Decision Flowchart

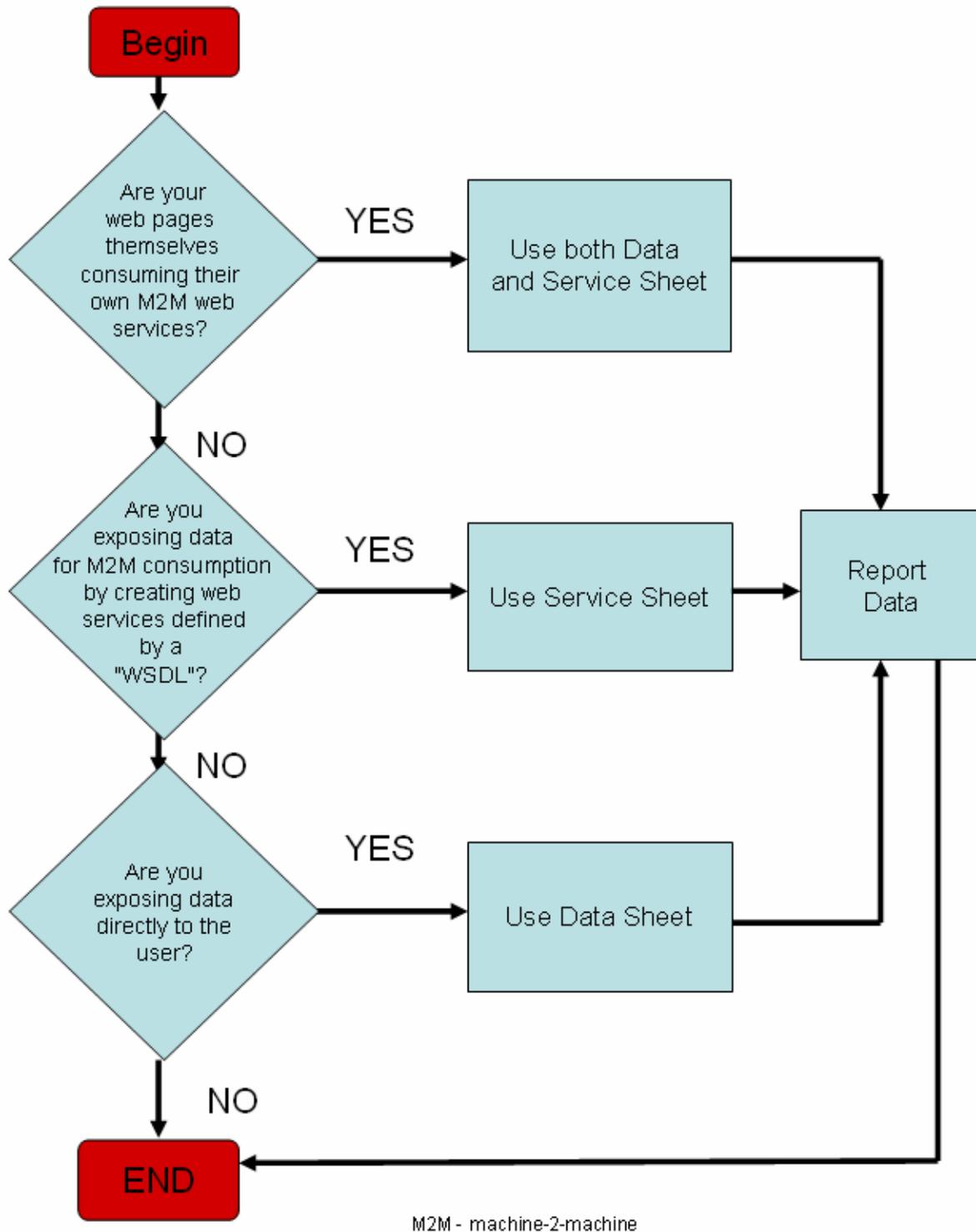


Figure 3 – Exposure Verification Tracking Sheet Decision Flowchart

## 6. Getting Started

After you have determined what you are exposing (data, service, or both), it is time to start doing the work of making it visible, accessible, and understandable.

You will need to use the NCES Services described in section 4 to register the different components of your data/service in order for a consumer to be able to use that information. To use NCES Capabilities, you should do the following:

- Review section 8 of this guide on the URLs of the web sites that will be needed as well as tips on how to gain access to those web sites.
- Acquire PKI and/or ECA certificates and NCES accounts
- Get the [NCES User's Guide](http://www.disa.mil/nces/nces_user_guide.html) ([http://www.disa.mil/nces/nces\\_user\\_guide.html](http://www.disa.mil/nces/nces_user_guide.html))
- Register on [DKO](https://www.us.army.mil) (<https://www.us.army.mil>)
- Request access to the [NCES Developer's Community](https://www.us.army.mil/suite/page/384284) (<https://www.us.army.mil/suite/page/384284>)

In addition, the following are lessons learned on things that will need to be done to get the process moving:

- Some SIPRNet sites require PKI Soft Certs that must be loaded on the computer from which you are trying to access the information – get these early in the process. *See section 6.1 to learn how to obtain a soft cert.*
- Need to know NCES Help Desk phone numbers: 1-800-447-2457, 614-692-3136, or DSN 850-3136.
- The Registry Operations personnel propagate the [MDR](#) information from low-to-high every two weeks unless requested—this could impact searches for information.
- Information in the NCES Services Registry ([UDDI](#)) is not propagated from low-to-high. To find information in the NCES Services Registry ([UDDI](#)) on a service, a search of both the high and low sides may be necessary.
- Start working early in the process on the security paperwork to get approval to operate.
- Enterprise Catalog, [MDR](#), and NCES Services Registry ([UDDI](#)) entries need to reflect what an unanticipated user would search on.
- Consumers of services need to ensure they get access to the services data via whatever means is listed in the services policy (policy should be posted in the [MDR](#)).

### 6.1 DoD PKI Certificates

If you work on DoD Government Furnished Equipment (GFE), then you are eligible to acquire three DoD PKI client certificates (one identity, one email signature, and one email encryption certificate). PKI client certificates issued by DoD may be obtained free of charge. DoD PKI certificates are available as software certificates (private keys stored in three \*.p12 files) or on Common Access Cards (private keys embedded in CAC). DoD Contractors may obtain CACs if their government sponsor deems it necessary.

If you do not work on DoD GFE, you will need to obtain ECA/IECA client certificates (identity, email signature and email encryption certificate). PKI client certificates issued by ECA/IECAs are available as software certificates only. Please note that ECA/IECA vendors require payment for PKI client certificates.

### **6.1.1 Obtaining DoD PKI Software Certificates**

To obtain a DoD PKI Software Certification, you will need to contact your Local Registration Authority (LRA). Your LRA may request that you complete [DD Form 2842](#). If so, please read the [DD Form 2842](#) Instructions.

**Air Force Users** may find their LRA at the following link (Restricted to \*.mil domain) <https://afpki.lackland.af.mil/html/lracontacts.asp> Locations which do not show a LRA may have a Trusted Agent (TA) available. Please contact [afpki.ra@lackland.af.mil](mailto:afpki.ra@lackland.af.mil) with specific physical location and organization that support is required and you will be sent a list of TA's at that location.

**Army Users** should contact the United States Army Registration Authority at (703) 892-7414 or at [army.ra@us.army.mil](mailto:army.ra@us.army.mil). The Army RA will review your requirements and assist you to locate a LRA or Trusted Agent (TA) in your geographic proximity.

**Navy/Marine Corps Users** may find their LRA at the following link (restricted to \*.mil and \*.gov domains): <https://infosec.navy.mil/PKI/lramain.html>

### **6.1.2 Obtaining ECA/IECA Certificates**

Please visit the following IASE link: <http://iase.disa.mil/pki/eca/> (lists the 3 steps to obtain an ECA/IECA certificate).

The next step in the process is the documentation of your efforts which will be covered in the next section.

## 7. How to Fill Out the Exposure Verification Tracking Sheet

### 7.1. Data

 <b>Data Exposure Verification Tracking Sheet for &lt;program&gt;</b>									
Key: <span style="border: 1px solid black; padding: 2px;">N</span> = Not Started <span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">I</span> = In-Progress <span style="background-color: #FFFF00; border: 1px solid black; padding: 2px;">R</span> = Progress at Risk <span style="background-color: #FF0000; border: 1px solid black; padding: 2px;">S</span> = Progress Stopped <span style="background-color: #ADD8E6; border: 1px solid black; padding: 2px;">A</span> = Objective Achieved <span style="border: 1px solid black; padding: 2px;">X</span> = Not Applicable									
Program Manager Telephone # E-Mail Address	Project POC Telephone # E-Mail Address						# of Objectives Achieved Since Previous Submission		
Web Page URL				Visible	Accessible		Understandable		
IT System DITPR Number				CD&D (1.a)	Policy (2.a)	Oper (2.b)	User (3.a)		Submission Date
Top Level JCA	Data Asset	Description		(Note: Use above 'Key' to assign values for columns below)				Issues/Comments	Exposure Start / Complete Date
(JCA Category)	Asset #1	Description #1							
	Asset #2	Description #2							
	Asset #n	Description #n							
(JCA Category)	Asset #1	Description #1							
	Asset #2	Description #2							
	Asset #n	Description #n							
(JCA Category)	Asset #1	Description #1							
	Asset #2	Description #2							
	Asset #n	Description #n							

<UNCLASSIFIED>

**Figure 4 – Data Exposure Verification Tracking Sheet**

Instructions on filling out each block of the Data Exposure Verification Sheet follows:

**Slide Title** Should be the name of the Program of Record (POR)/System of Record (SOR) being exposed in the format: "Data Exposure Verification Tracking Sheet for *name of POR/SOR*."

**Program Manager / Telephone # / E-Mail Address** Enter the name, phone number, and E-Mail address of the person responsible for management of the POR/SOR.

**Project POC / Telephone # / E-Mail Address** Enter the Point of Contact (POC) name, phone number, and E-Mail Address of the person who will be responsible for updating and submitting the Exposure Verification Sheets.

**Web Page URL** Enter the web page Uniform Resource Locator (URL) address of the data being exposed.

**IT System / DITPR Number** Enter the name of the primary system on which the POR/SOR is running on and the id number of that system registered in the [DoD Information Technology Portfolio Repository \(DITPR\)](#).

**Top Level JCA** Joint Capability Area (JCA)s are collections of similar capabilities grouped at a high level in order to support decision making, capability delegation, and analysis. The current list of Top Level JCAs can be found in the table on the right. Select the JCA(s) that applies to your POR/SOR and enter it on the sheet. This information can typically be found in key program documents such as the Capability Development Document (CDD).

Top Level Joint Capability Areas
Force Application
Influence
Command and Control
Net-Centric
Battlespace Awareness
Protection
Logistics
Force Support
Corporate Management and Support

**Data Asset** Enter the name of the data asset registered in the Enterprise Catalog. The [DoD Net-Centric Data Strategy](#) defines a data asset as any entity that is composed of data. For example, a database is a data asset that contains data records; e.g., system or application output files, databases, documents, or web pages.

**Description** Enter a short description of the data being exposed in this block.

**# of Objectives Achieved Since Previous Submission** This block is a numerical count of the number of achieved areas relative to the previous submission of the slide.

**Submission Date** Self Explanatory.

**Issues/Comments** Include comments if anything needs to be further explained on the slide.

**Exposure Start / Complete Date** Enter the dates of the beginning and end of the exposure effort in the following format: DD MMM YY.

For each objective on the Data Exposure Verification Tracking Sheet, the tables in this part of the guide show what is required for each status milestone. For situations that are not covered by this guide, please place notes in the issues block of the slide.

### 7.1.1. Data Visible (Federated Search) Criteria

"Visible. Able to be seen, detected, or distinguished and to some extent characterized by humans and/or IT systems, applications, or other processes." <sup>4</sup>

### Content Discovery and Delivery (CD&D)

	Status	Data Visible – CD&D Criteria
<b>A</b>	<b>Objective Achieved</b>	1. <a href="#">DDMS</a> information entered in an Enterprise Catalog 2. Data can be found by a Federated Search
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

Information on how to enter items into the NCES Enterprise Catalog can be found on the NCES Developer Web Site – <https://www.us.army.mil/suite/page/384284> in the Content Discovery section. Note: You will need an AKO/DKO account to access this web site.

#### 7.1.2. Data Accessible (User) Criteria

"Accessible. A data asset is accessible when a human, system, or application may retrieve the data within the asset. Data assets may be made accessible by using shared storage space or web services that expose the business or mission process that generates data in readily consumable forms."<sup>4</sup>

#### Policy

	Status	Data Accessible – Policy Criteria
<b>A</b>	<b>Objective Achieved</b>	If your data is not accessible to all users you must present the user with written policy on how to gain access to the site within two clicks that is understandable by anticipated and unanticipated users
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

### Operational (Transparent Access)

	Status	Data Accessible – Operational Criteria
<b>A</b>	<b>Objective Achieved</b>	NCES Federated Search results provide active link that when it is selected provides access to the website without requiring the user to enter credentials (i.e. username, password) or by exercising policy (e.g. request access, obtain login)
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

### 7.1.3. Data Understandable Criteria

"Understandable. Capable of being comprehended in terms of subject, specific content, relationships, sources, methods, quality, spatial and temporal dimensions, and other factors." <sup>4</sup>

### User Interaction

	Status	Data Understandable – User Criteria
<b>A</b>	<b>Objective Achieved</b>	The keywords entered in the DoD Discovery Metadata Specification ( <a href="#">DDMS</a> ) record in the Enterprise Catalog must reflect common terms used by the user <ul style="list-style-type: none"> <li>– Search terms/keywords appropriate for Mission area or data type</li> <li>– Described data understandable to both anticipated and unanticipated user</li> <li>– Mission data maps back to search terms</li> </ul>
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

7.2. Service



## Service Exposure Verification Tracking Sheet for <program>

Key: N = Not Started   I = In-Progress   R = Progress at Risk   S = Progress Stopped   A = Objective Achieved   X = Not Applicable

Program Manager Telephone # E-Mail Address		Project POC Telephone # E-Mail Address		Visible		Accessible		Understandable		# of Objectives Achieved Since Previous Submission		
MDR Namespace		IT System DITPR Number		MDR (1.a)	UDDI (1.b)	UDDI (2.a)	Policy (2.b)	MDR (3.a)	COI (3.b)	Submission Date		
Top Level JCA	Service Name	Service Type	MDR Submission Pkg Name	Service Description	(Note: Use above Key to assign values for columns below)						Issues/Comments	Exposure Start / Complete Date
(JCA Category)	Service Name #1											
	Service Name #2											
	Service Name #n											
(JCA Category)	Service Name #1											
	Service Name #2											
	Service Name #n											
(JCA Category)	Service Name #1											
	Service Name #2											
	Service Name #n											

<UNCLASSIFIED>

**Figure 5 – Service Exposure Verification Tracking Sheet**

Instructions on filling out each block of the Service Exposure Verification Sheet follows:

**Slide Title** Should be the name of the POR/SOR being exposed in the format: "Service Exposure Verification Tracking Sheet for *name of POR/SOR*."

**Program Manager / Telephone # / E-Mail Address** Enter the name, phone number, and E-Mail address of the person responsible for management of the POR/SOR.

**Project POC / Telephone # / E-Mail Address** Enter the Point of Contact (POC) name, phone number, and E-Mail Address of the person who will be responsible for updating and submitting the Exposure Verification Sheets.

**MDR Namespace** Enter the name of the [MDR](#) Governance Namespace under which the POR/SOR is registered.

**IT System / DITPR Number** Enter the name of the primary system on which the POR/SOR is running on and the id number of that system registered in the [DoD Information Technology Portfolio Repository \(DITPR\)](#).

**Top Level JCA** JCAs are collections of similar capabilities grouped at a high level in order to support decision making, capability delegation, and analysis. The current list of Top Level JCAs can be found in the table on the right. Select the JCA(s) that applies to your POR/SOR and enter it on the sheet. This information can typically be found in key program documents such as the Capability Development Document (CDD).

Top Level Joint Capability Areas
Force Application
Influence
Command and Control
Net-Centric
Battlespace Awareness
Protection
Logistics
Force Support
Corporate Management and Support

**Service Name** Enter the name of the service as it is registered in the NCES Services Registry ([UDDI](#)). If the name is unknown because it has not been determined or entered into the registry, enter TBD in this block.

**Service Type** Enter the type of service that is being exposed (e.g. [Web Service](#), [RSS](#), [KML](#), or [GeoRSS](#).)

**MDR Submission Pkg Name** Enter the name of the submission package as it was entered into the [MDR](#). If the name is unknown because it has not been determined or not yet entered into the registry, enter TBD in this block.

**Service Description** Enter a short description of the service being exposed in this block.

**# of Objectives Achieved since previous submission** This block is a numerical count of the number of achieved areas relative to the previous submission.

**Date Submitted** Self Explanatory.

**Issues/Comments** Include comments if anything needs to be further explained on the slide.

**Exposure Start / Complete Date** Enter the dates of the beginning and end of the exposure effort in the following format: DD MMM YY.

For each objective on the Service Exposure Verification Tracking Sheet, the tables in this part of the guide show what is required for each status milestone. For situations that are not covered by this guide, please place notes in the issues block of the slide.

### 7.2.1. Service Visible (Registered and Discoverable) Criteria

"Visible. Able to be seen, detected, or distinguished and to some extent characterized by humans and/or IT systems, applications, or other processes."<sup>4</sup>

#### DoD Metadata Registry (MDR)

	Status	Service Visible - MDR Criteria
<b>A</b>	<b>Objective Achieved</b>	WSDLs, XML Schema Definitions (XSDs), and XML instances will be registered in <a href="#">MDR</a>
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

#### Universal Description, Discovery and Integration ([UDDI](#)) – NCES Services Registry

	Status	Service Visible – UDDI Criteria
<b>A</b>	<b>Objective Achieved</b>	Operational end points registered in the NCES Services Registry ( <a href="#">UDDI</a> ) by referencing the WSDL in the <a href="#">MDR</a> (note: WSDL must first be registered in the <a href="#">MDR</a> )
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

### 7.2.2. Service Accessible (Developer Access) Criteria

"Accessible. A data asset is accessible when a human, system, or application may retrieve the data within the asset. Data assets may be made accessible by using shared storage space or web services that expose the business or mission process that generates data in readily consumable forms."<sup>4</sup>

**UDDI (Active Links – Endpoints & WSDL)**

	Status	Service Accessible – UDDI Criteria
<b>A</b>	<b>Objective Achieved</b>	1. NCES Services Registry ( <a href="#">UDDI</a> ) registered service end-points provide transparent machine-to-machine access to operational data at the targeted security enclave 2. NCES Services Registry ( <a href="#">UDDI</a> ) registered service links to accessible WSDL definition in the <a href="#">MDR</a>
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

**Policy**

	Status	Service Accessible – Policy Criteria
<b>A</b>	<b>Objective Achieved</b>	1. Service Provider has written policy registered in the DoD <a href="#">MDR</a> listing actions necessary to gain transparent machine-to-machine access to services 2. Policy information as well as the steps listed to request access to the service made clear for unanticipated developer
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

For the time being the [MDR](#) is a good place to store these policies; however, when the NCES Services Registry ([UDDI](#)) can store files (current version can not), it may be more appropriate to place the policies within the NCES Services Registry ([UDDI](#)), especially if the policies pertain to web services. If the policy is placed in the [MDR](#), a good practice would be to place a note in the NCES Services Registry ([UDDI](#)) letting people know where to find it.

The next version of the NCES Services Registry ([UDDI](#)) will be able to store files. This version is scheduled to be fielded in early 2008.

### 7.2.3. Service Understandable Criteria

"Understandable. Capable of being comprehended in terms of subject, specific content, relationships, sources, methods, quality, spatial and temporal dimensions, and other factors."<sup>4</sup>

#### DoD Metadata Registry (MDR)

	Status	Service Understandable – MDR Criteria
<b>A</b>	<b>Objective Achieved</b>	Service provider schemas and supporting documentation registered in <a href="#">MDR</a>
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

#### Community of Interest (COI)

	Status	Service Understandable – COI Criteria
<b>A</b>	<b>Objective Achieved</b>	Service schemas conform to standard (COI approved) vocabulary
<b>I</b>	<b>In-Progress</b>	Progress towards this objective is started and there are no reasons to believe that the objective will not be met in the required timeframe
<b>Y</b>	<b>Progress at Risk</b>	There is a reason to believe that the objective will not be met – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>S</b>	<b>Progress Stopped</b>	No work towards exposure is currently being done due to some issue – include reason(s) in the issues block of the Exposure Verification Tracking Sheet
<b>N</b>	<b>Exposure Not Started</b>	Exposure work has not yet started

## 7.3. Examples

### 7.3.1. Data

The following example uses the exposure of the Maritime Domain Awareness (MDA) data. Below is the Data Exposure Verification Tracking Sheet slide for MDA data.

 <b>Data Exposure Verification Tracking Sheet for Maritime Domain Awareness (MDA)</b>										
Key: <span style="border: 1px solid black; padding: 2px;">N</span> = Not Started <span style="background-color: #90EE90; border: 1px solid black; padding: 2px;">I</span> = In-Progress <span style="background-color: #FFFF00; border: 1px solid black; padding: 2px;">R</span> = Progress at Risk <span style="background-color: #FF0000; border: 1px solid black; padding: 2px;">S</span> = Progress Stopped <span style="background-color: #ADD8E6; border: 1px solid black; padding: 2px;">A</span> = Objective Achieved <span style="border: 1px solid black; padding: 2px;">X</span> = Not Applicable										
Program Manager	Joe Smith	Project POC	Fred Rubble				# of Objectives Achieved Since Previous Submission		2	
Telephone #	DSN 622-1234	Telephone #	DSN 123-8754							
E-Mail Address	joe@usa.mil	E-Mail Address	fred@usa.mil							
Web Page URL	https://mda.spawar.navy.mil			Visible	Accessible	Understandable				
IT System	MDA	CD&D (1.a)	Policy (2.a)	Oper (2.b)	User (3.a)		Submission Date		1 Jul 07	
DITPR Number	9999									
Top Level JCA	Data Asset	Description	(Note: Use above 'Key' to assign values for columns below)			Issues/Comments		Exposure Start / Complete Date		
Force Application	MDA AIS	Converts MDA DS COI messages containing Automated Identification System information to Google Keyhole Markup Language	A	A	A	A		1 Apr 07	30 Jun 07	

Federated Search on "MDA AIS" produces results with an URL as shown below – Visible CD&D Objective Achieved.



The screenshot shows the GES/DefenseOnline search results for the query "MDA AIS". The search results are displayed in a list format. The third result is highlighted with a blue border, indicating it is the relevant result. The highlighted result is titled "MDA DS COI Google Maps Mediation Service" and includes the following details:

- Description:** Maritime Domain Awareness Data Sharing Community of Interest (MDA DS COI) Google Maps Mediation Service. Google Maps Mediation Service converts MDA DS COI messages containing Automated Identification System (AIS) information to Google Keyhole Markup Language (KML).
- URL:** <https://mda.spawar.navy.mil>
- Date:** 2007-08-08T06:24:22Z
- Relevance:** 100
- Provider:** Messaging/Enterprise Catalog

The page also shows other search results, including "UNCLASSIFIED" and "NAVY ROLE IN GLOBAL WAR ON TERRORISM (GWOT) BACKGROUND AND ISSUES...". The search interface includes a navigation menu, a search bar, and a status bar at the bottom.

Selecting the link provided by the Federated Search requires the user to enter their Common Access Card (CAC) credentials. Upon verifying the CAC, access to the web site is achieved as shown in the series of examples below. **Accessible – Operational Objective Achieved.** Policy is clear because only CAC credentials are required to access the site. **Accessible Policy Objective Achieved.**

The screenshot shows a Microsoft Internet Explorer browser window displaying a search results page for 'https://mda.spawar.navy.mil/'. The search results list several items, with the third item, 'MDA DS COI Google Maps Mediation', circled in blue. A 'Client Authentication' dialog box is overlaid on the page, prompting the user to select a certificate for identification. A blue arrow points from the 'Client Authentication' dialog box to the circled search result.

**Client Authentication**

Identification

The Web site you want to view requests identification. Select the certificate to use when connecting.

WAITE.DAV  
WAITE.DAV

More Info... View Certificate...

OK Cancel

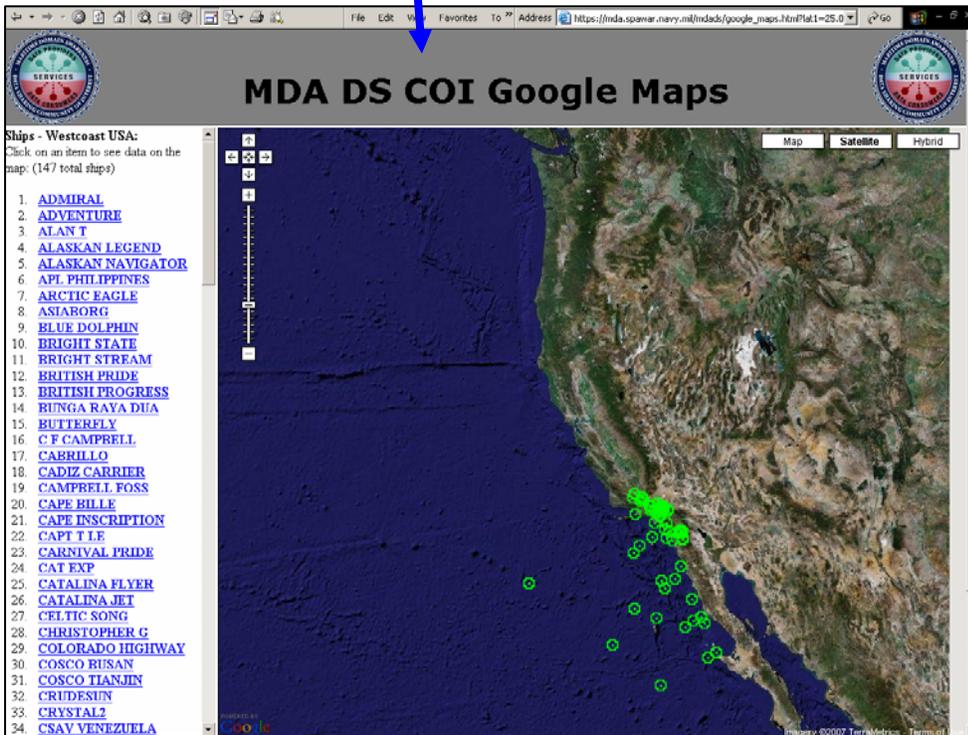
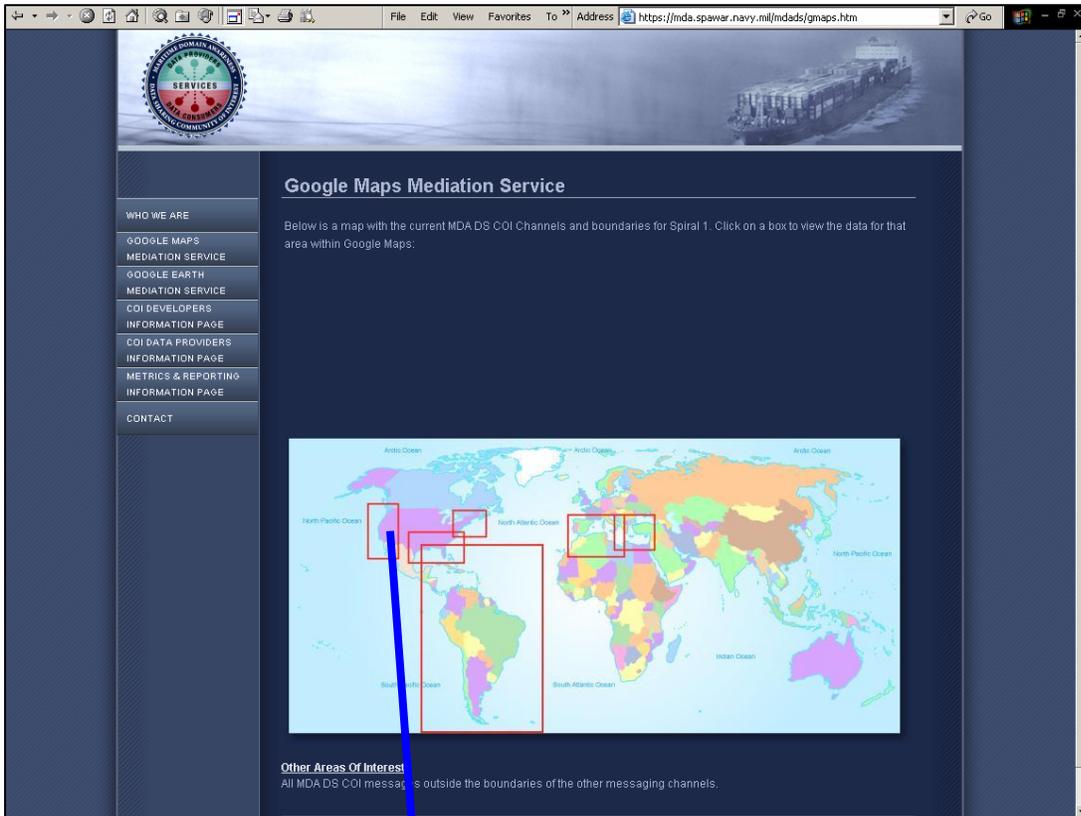
**MDA DS COI Google Maps Mediation**

Description: Maritime Domain Awareness MDA DS COI messages containing Auto https://mda.spawar.navy.mil

Date: 2007-08-08T06:24:22Z

Relevance: 100

Provider: Messaging/Enterprise Catalog



Working with the COI, it was determined that the keywords used for searching were appropriate for the mission area and data type, data is understandable, and mission data maps back to search terms **Understandable User Objective Achieved.**

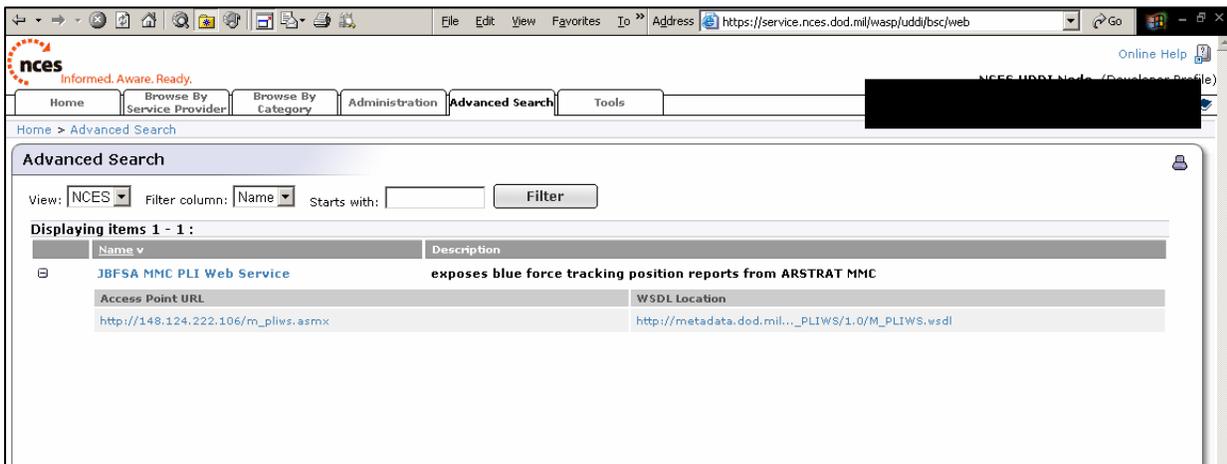
### 7.3.2. Service

 <b>Service Exposure Verification Tracking Sheet for JBFSA MMC</b>												
Key: <b>N</b> = Not Started <b>I</b> = In-Progress <b>R</b> = Progress at Risk <b>S</b> = Progress Stopped <b>A</b> = Objective Achieved <b>X</b> = Not Applicable												
Program Manager	Joe Smith	Project POC	Fred Rubble		Visible		Accessible		Understandable		# of Objectives Achieved Since Previous Submission	7
Telephone #	DSN 622-1234	Telephone #	DSN 123-6754									
E-Mail Address	Joe@usa.mil	E-Mail Address	Fred@usa.mil									
MDR Namespace	BFT	IT System	JBFSA MMC		MDR (1.a)	UDDI (1.b)	UDDI (2.a)	Policy (2.b)	MDR (3.a)	COI (3.b)	Submission Date	24 Aug 07
		DITPR Number	9999		(Note: Use above Key to assign values for columns below)							
Top Level JCA	Service Name	Service Type	MDR Submission Pkg Name	Service Description							Issues/Comments	Exposure Start / Complete Date
Battlespace Awareness	JBFSA MMC PLI Web Service	Web Service	MMC AssociationData	Blue force location data	A	A	A	I	A	I	Policies documented, but not yet posted to MDR. COI IES not final.	1 Jul 07

The following example uses the exposure of the Joint Blue Force Situational Awareness (JBFSA) Mission Management Center (MMC) PLI Web Service. Below is the Service Exposure Verification Tracking Sheet slide for JBFSA.

The operational end point is registered in the NCES Services Registry ([UDDI](#)) by referencing the WSDL in the [MDR](#) - **Visible** - [UDDI Objective Achieved](#).

As demonstrated by an integrator (not shown) Web Service end-points provide transparent machine-to-machine access. WSDL registered in the Services Registry ([UDDI](#)) provides a link to the WSDL in the [MDR](#) - **Accessible** - [UDDI Objective Achieved](#).



WSDL registered in the DoD [MDR](#) – **Visible** – [MDR Objective Achieved](#).

Service Provider schemas and supporting documentation are registered in the [MDR](#) – **Understandable** – [MDR Objective Achieved](#) but since the note on the Exposure Verification Tracking Sheet says COI not final – **Understandable** – [COI Objective Exposure In-Progress](#).

The screenshot shows the DoD METADATA REGISTRY v6.1 AND CLEARINGHOUSE interface. The search bar is set to "All Data" and "Advanced Search". The "View By Namespace" section is active, displaying a list of namespaces. The "BFT: Blue Force Tracking" namespace is selected and circled in black. To the right, the "Namespace Details" for BFT are shown:

Namespace Details	
Name:	Blue Force Tracking
Description:	Blue Force Tracking Community of Interest
Abbreviation:	BFT
Parent Namespace:	DODENT
Webpage:	https://gesportal.dod.mil/sites/BFTCOIPilot/default.aspx
Network:	NIPRNET
Status:	Developmental
URL Identifier:	BFT

The screenshot shows the DoD METADATA REGISTRY v6.1 AND CLEARINGHOUSE interface. The search bar is set to "All Data" and "Advanced Search". The "Search Results" section is active, displaying search criteria and a list of results. The search criteria are:

- Information Resource Types: Submission Package
- Governance Namespaces: BFT
- Download: XML | CSV

The search results show 1 - 2 of 2 records:

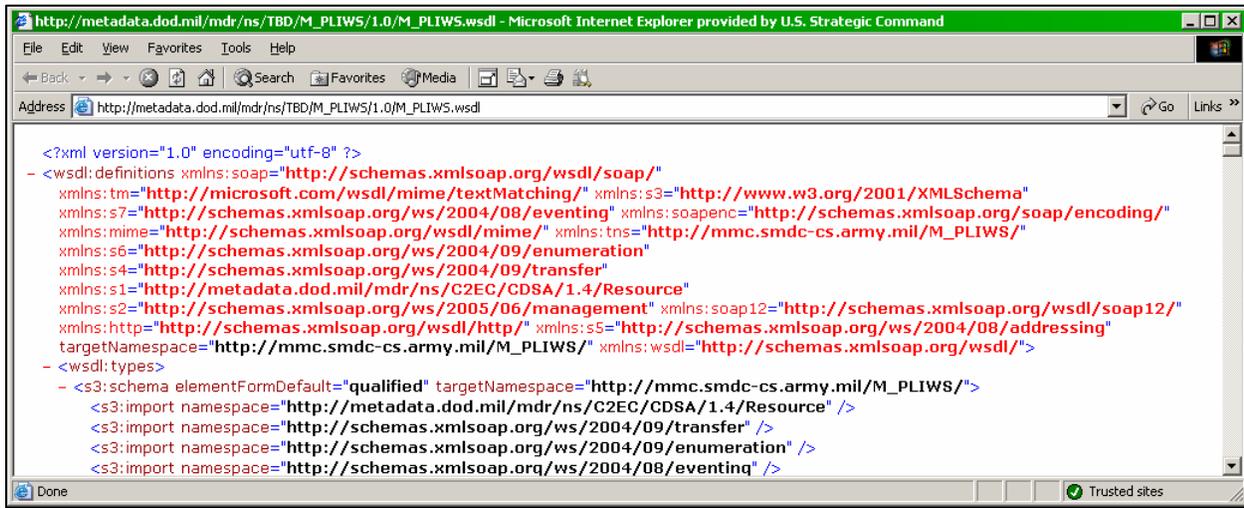
- BFT\_COI\_IES (Submission Package, v0.2, Developmental, 03/12/2007)
- MMCAssociationData (Submission Package, v1.0, Developmental, 07/17/2007)  
MMC Association Data Schema

The screenshot shows the DoD METADATA REGISTRY v6.1 AND CLEARINGHOUSE interface. The search bar is set to "All Data" and "Advanced Search". The "Information Resource (IR) Details" section is active, displaying details for the "MMC PLIWS WSDL" resource:

Information Resource (IR) Details	
Name:	MMC PLIWS WSDL
Average Rating:	No User Ratings found.
Definition:	MMC PLI Web Service WSDL v1.1
Comment:	This WSDL defines the web services supported by the MMC PLI Web Service
Version:	1.1
Namespace:	To Be Determined
Status:	Developmental
Type:	WSDL
Security Classification:	Unclassified
Context:	No value provided.
Creator:	Dan Stephens (daniel.stephens@smdc-cs.army.mil)
Submitter:	Dan Stephens (daniel.stephens@smdc-cs.army.mil)
Creation Date:	10/18/2007
Effective Date:	09/15/2007
Update Date:	

The "Relationships" section shows:

Relationships		
MMC PLIWS WSDL (v1.1)	is a newer version of	MMC PLIWS WSDL (v1.0)
MMC PLIWS WSDL (v1.1)	has the member	MMC PLIWS WSDL (v1.1)



The screenshot below is from the [COI Directory](#) in the [MDR](#). Using the information located there allows an organization to begin to determine if the service schemas conform to standard (COI approved) vocabulary.

**DoD METADATA REGISTRY v6.1 AND CLEARINGHOUSE**  
 the authoritative source for structural metadata

Search  for   Advanced Search

You are logged in as David Waite. [Logout](#)

**COI Details**

**Name:** Blue Force Tracking (BFT)  
**Status:** Effective

Information Exchange Standard that facilitates BFT across Joint and Allied/Coalition forces to effectively ensure that data is visible, accessible, trusted, understandable and in accordance with the DoD Net-Centric Data Strategy and Directive 8320.2.

**Collaborative Space:** <https://gesportal.dod.mil/sites/BFTCOIPilot/default.aspx>

**MDR Namespace(s):**

**Domain Sponsor(s):** Battlespace Awareness (WMA)

**"Other" Sponsoring Organization:**

**Lead Name:** LTC Tony Krogh  
**Lead Organization:** HQDA G-3  
**Lead Phone Number:**

**Lead Email:** [anthony-krogh@us.army.mil](mailto:anthony-krogh@us.army.mil)  
**Chair Name:** SES Mr. James Cooke  
**Chair Organization:** HQDA G-3 BC  
**Chair Phone Number:** n/a  
**Chair Email:** n/a

**POC Name:** Salvatore F La Forgia  
**POC Organization:** HQDA G-3/PEO C3T  
**POC Phone Number:** (732) 427-2730  
**POC Email:** [salvatore.f.laforgia@us.army.mil](mailto:salvatore.f.laforgia@us.army.mil)  
**Co-Chair Name:** SL Mr. David Green  
**Co-Chair Organization:** HQMC C4  
**Co-Chair Phone Number:** 703-693-3462  
**Co-Chair Email:**

**2nd POC Name:** LTC Lem Thomas  
**2nd POC Organization:** USJFCOM J87  
**2nd POC Phone Number:** (757) 836-4169  
**2nd POC Email:** [lemuel.thomas@jfc.com](mailto:lemuel.thomas@jfc.com)

Questions or Suggestions? [Click here to send feedback and comments.](#)  
[Metadata Registry Privacy Notice](#)  
[Metadata Registry Foreign Access Notice](#)

## 8. How to Verify Exposure Verification Tracking Sheet Compliance

### 8.1 Verification

To verify net-centric compliance IAW the Exposure Verification Tracking Sheets, you will need to access certain web sites and search for the items for each data/service being validated. Each Exposure Verification Tracking Sheet should contain the necessary information to validate net-centric exposure. Each table in sections [7.1](#) and [7.2](#) of this guide lists what is required to have each objective achieved. A quick look checklist can also be found at [Enclosure D](#). If the criterion listed in the tables is met, then you have validated the objective as being achieved.

The following web sites will assist in validating net-centric compliance. Assistance on getting access to NCES Services (UDDI, MDR, and Federated Search) can be found in the [Net-Centric Enterprise Services User Guide](#) at [http://www.disa.mil/nces/NCES\\_UG\\_Final\\_v1\\_1.pdf](http://www.disa.mil/nces/NCES_UG_Final_v1_1.pdf).

Additional information on how to use the [NCES Service Registry \(UDDI\)](#) can be found in the [Service Discovery Systinet 6.0+ User Guide](#) on that page's "Online Help" link.

- NCES Service Registry (UDDI) – NOTE: *(requires registration)*
  - NIPRNet <https://service.nces.dod.mil/wasp/uddi/bsc/web>
  - SIPRNet <https://service.nces.dod.smil.mil/wasp/uddi/bsc/web> - Note: *Also requires PKI soft cert for access*

**Note:** *Users are required to be manually entered into the LDAP before the website allows access, a requirement that is not listed on the website. You must contact the NCES Help Desk to get registered.*
  
- Metadata Registry (MDR) - NOTE: *(requires registration)*
  - NIPRNet <https://metadata.dod.mil> – Note: As of version 6.1 CAC login is enabled if you have a AKO/DKO account set up.
  - SIPRNet <https://metadata.dod.smil.mil>

**Note:** *Attempting to use the same user name for an MDR login on both NIPRNet and SIPRNet will result in a registration error. Use different login names for each one.*
  
- Federated search capability, such as - NOTE: *(requires registration)*
  - NIPRNet <https://portal.nces.dod.mil/NCES.portal> (select Content Discovery/Delivery – Enterprise Search)  
<https://gesportal.dod.mil/default.aspx> (select NCES Search)
  - SIPRNet <https://www.dko.dod.smil.mil>  
<http://search-eng.csd.disa.smil.mil/mse/>

**Note:** [Intelink](#) on SIPRNet is not currently a Federated Search. That capability is planned to be added to [Intelink](#) in early 2008.
  
- DoD Information Technology Standards Registry current Baseline Release - NOTE: *(requires registration)*
  - NIPRNet <https://disronline.disa.mil>
  - SIPRNet <http://disronline.disa.smil.mil/a/DISR>

- Communities of Interest (COI) Web Page - NOTE: *(requires registration)* As of 19 December 2007 the COI Web Page was moved to the MDR web pages.
  - NIPRNet <https://metadata.dod.mil> – Note: As of version 6.1 CAC login is enabled if you have an AKO/DKO account set up.
  - SIPRNet <https://metadata.dod.smil.mil>
- DoD Discovery Metadata Specification (DDMS)
  - NIPRNet <http://metadata.dod.mil/mdr/irs/DDMS/>
  - SIPRNet <http://metadata.dod.smil.mil/mdr/irs/DDMS/>
- DoD Information Technology Portfolio Repository (DITPR) - NOTE: *(requires registration)*
  - NIPRNet <https://ditpr.dod.mil/>
- Vocabulary OneSource (can be used to check COI vocabulary)
  - NIPRNet <https://gcic.af.mil/vocabulary/>  
NOTE: *(requires registration)* This is a web-enabled tool which can be accessed with an AF Global Cyberspace Integration Center (GCIC) toolset account. To request an account go to <https://gcic.af.mil/toolset/RequestNewUser.asp>. Once you are notified your toolset account is established, contact the Vocabulary Office at DSN 575-6273/CML 757-225-6273 or [GCIC.RINIV@langley.af.mil](mailto:GCIC.RINIV@langley.af.mil) to request access to OneSource.

## 8.2 Lessons Learned

In addition to the web sites listed in the previous section, the following are lessons learned from previous evaluators on what is required to determine net-centricity:

- Get accounts for access to all services/data that are being exposed if possible in order to evaluate end-to-end.
- Some SIPRNet sites require PKI soft certs that must be loaded on the computer from which you are trying to access the information— get these early in the process. *See section 6.1 on how to obtain a soft cert.*
- Need to know NCEC Help Desk phone numbers: 1-800-447-2457, 614-692-3136, or DSN 850-3136.
- Get help desk POCs for all services/data being evaluated.
- The Registry Operations personnel propagate the [MDR](#) information from low-to-high every two weeks unless requested—this could impact searches for information.
- Information in the NCEC Services Registry ([UDDI](#)) is not propagated from low-to-high. To find information in the NCEC Services Registry ([UDDI](#)) on a service, a search of both the high and low sides may be necessary.

## 9. Warning on Foreign Nationals Use of the DISA Metadata Registry (MDR)

The following note is posted on the DISA [MDR](#) log-in web page.

(<https://metadata.dod.mil/mdr/login.htm>)

**Foreign Disclosure Notification** Please be advised that the unclassified NIPRNet instance of the DoD Metadata Registry (MDR) user base includes sponsored users from outside of the Department of Defense, including non-US citizens (NATO users – see [NATO-DISA MDR MOU](#)). Accordingly, the NIPRNet MDR should be used only for publishing metadata that is unclassified and not subject to formal controls or special handling caveats.

## ENCLOSURE A

### **GLOSSARY**

**Accessible.** A data asset is accessible when a human, system, or application may retrieve the data within the asset. Data assets may be made accessible by using shared storage space or services that expose the business or mission process that generates data in readily consumable forms.

**Authoritative Source.** A source of data or information that is recognized by members of a COI to be valid or trusted because it is considered to be highly reliable or accurate or is from an official publication or reference (e.g., the United States (U.S.) Postal Service is the official source of U.S. mailing ZIP codes).

**Community of Interest (COI).** A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges.

**Data.** A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Data and information are equivalent terms for the purposes of this guide.

**Data Asset.** Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset. A human, system, or application may create a data asset.

**Domains.** In this guide, domains are subsets of Mission Areas and represent a common collection of related, or highly dependent, information capabilities and services. Managing these related information capabilities and services within domains improves coordination, collaboration, integration, and consistency of processes and interfaces for information sharing.

**Enterprise.** Refers to the Department of Defense, its organizations, and related Agencies.

**Enterprise Information Environment Mission Area.** The Department of Defense's Mission Area responsible for managing the part of the DoD portfolio known as the enterprise information environment (EIE), which is the common, integrated computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, or that assure, local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks, and wide area networks. The EIE is also composed of GIG assets that operate as, or that assure, end user devices, workstations, and servers that provide local, organizational, regional, or global computing capabilities. The EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in

the GIG. The EIE includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG.

**Global Information Grid (GIG)**. The globally connected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

**Information Capability**. The ability to consume and generate information in the form of data assets by performing a specific task using IT and/or NSS.

**Information Technology (IT)**. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used directly by the DoD Component or is used by a contractor under a contract with the DoD Component which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related sources. It also includes NSS. Notwithstanding the above, the term “information technology” does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

**Law, Policy, or Security Classification**. For this guide, the pertinent statutory and regulatory authority dealing with data assets includes, but is not limited to: personal information, intelligence information, medical information, information on a non-DoD person, and classified information.

**Metadata**. Information describing the characteristics of data; data or information about data; or descriptive information about an entity’s data, data activities, systems, and holdings. For example, discovery metadata is a type of metadata that allows data assets to be found using enterprise search capabilities.

**Metadata Registry**. Repository of all metadata related to data structures, models, dictionaries, taxonomies, schema, and other engineering artifacts that are used to support interoperability and understanding through semantic and structural information about the data. A federated metadata registry is one in which multiple registries are joined electronically through a common interface and exchange structure, thereby effecting a common registry.

**Mission Area**. A defined area of responsibility with functions and processes that contribute to mission accomplishment.

**Net-Centric**. Relating to or representing the attributes of net-centricity. Netcentricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms.

Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-Centric capabilities enable network-centric operations and NCW.

**Semantic Metadata.** Information about a data asset that describes or identifies characteristics about that asset that convey meaning or context (e.g., descriptions, vocabularies, taxonomies).

**Shared Space.** Storage on a file server or in electronic media that is addressable by multiple users or COIs. Also, services that are made available to the enterprise that expose the business or mission processes that generate data in readily consumable forms.

**Structural Metadata.** Information provided about a data asset that describes the internal structure or representation of a data asset (e.g., database field names, schemas, web service tags).

**Understandable.** Capable of being comprehended in terms of subject, specific content, relationships, sources, methods, quality, spatial and temporal dimensions, and other factors.

**Users.** Humans, systems, and applications that create, find, access, and exploit data. Also known as consumers and producers, or publishers and subscribers. System developers are also considered to be users. For this guide, users may be expected and planned for, or unanticipated and not planned for.

**Visible.** Able to be seen, detected, or distinguished and to some extent characterized by humans and/or IT systems, applications, or other processes.

**Web Services.** A standardized way of integrating web-based applications using open standards over an Internet Protocol backbone. Web services allow applications developed in various programming languages and running on various platforms to exchange data without intimate knowledge of each application's underlying IT systems.

## ENCLOSURE B

### **REFERENCES**

1. [DODD 4630.05, 5 May 2004](#), “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”
2. [DODD 5000.1](#), 12 May 2003, “The Defense Acquisition System”
3. [DODD 8100.1](#), 19 September 2002, “Global Information Grid (GIG) Overarching Policy”
4. [DODD 8320.02](#), 2 December 2004, “Data Sharing in a Net-Centric Department of Defense”
5. [DODI 4630.8](#), 30 June 2004, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”
6. [DODI 5000.2](#), 12 May 2003, “Operation of the Defense Acquisition System”
7. [CJCSM 3170.01C](#), 1 May 2007, “Operation of the Joint Capabilities Integration and Development System”
8. [CJCSI 3170.01F](#), 1 May 2007, “Joint Capabilities Integration and Development System”
9. [CJCSI 6212.01D](#), 8 March 2006, "Interoperability and Supportability of Information Technology and National Security Systems"
10. [Net-Centric Operations and Warfare \(NCOW\) Reference Model \(RM\)](#)
11. [DOD Architecture Framework \(DODAF\)](#)
12. [DOD Chief Information Officer Memorandum, 9 May 2003, “DOD Net-Centric Data Strategy”](#)
13. "[DOD Net-Centric Services Strategy](#)", March 2007

## ENCLOSURE C

### **EXPOSURE STATUS CRITERIA**

#### **DATA**

##### **Visible**

- Content Discovery and Delivery (CD&D)
  - DoD Discovery Metadata Specification ([DDMS](#)) entry in an Enterprise Catalog
  - Content search function that federates to NCES Federated search

##### **Accessible**

- Policy
  - Data Provider has written policy listing actions necessary to gain transparent access to data via
    - User level credentials or,
    - System level credentials or,
    - Trust relationship (Access Control List).
  - Policy made clear for unanticipated user (e.g. available from Federated Search)
    - POC for access/login request within 2 clicks
- Operational (Transparent Access)
  - Transparent user access to operational data within the targeted security enclave
    - NCES Federated Search results provide active link (e.g. URL)

##### **Understandable**

- User Interaction
  - Search terms/keywords appropriate for Mission area or data type
  - Described data understandable to both anticipated and unanticipated user
  - Mission data maps back to search terms

## **EXPOSURE STATUS CRITERIA**

### **SERVICE**

#### **Visible**

- DoD Metadata Registry ([MDR](#))
  - Registration of WSDLs, XML Schema Definitions (XSDs), and XML instances
- Universal Description, Discovery and Integration ([UDDI](#)) – NCES Services Registry
  - Service instance registered by provider and discoverable by developer within targeted enclave

#### **Accessible**

- [UDDI](#) (Active Links – Endpoints & WSDL)
  - NCES Services Registry ([UDDI](#)) registered service end-points provide transparent machine-to-machine access to operational data at the targeted security enclave
  - NCES Services Registry ([UDDI](#)) registered service links to accessible WSDL definition in [MDR](#)
- Policy
  - Service Provider has written policy listing actions necessary to gain transparent machine-to-machine access to services via
    - User level credentials or,
    - System level credentials or,
    - Trust relationship, service level agreements.
  - Policy made clear for unanticipated developer
    - Policy information registered in [MDR](#)
    - Steps listed to request access to service

#### **Understandable**

- DoD [MDR](#)
  - Service Provider schemas and supporting documentation registered in [MDR](#)
- Community of Interest (COI)
  - Service schemas conform to standard (COI approved) vocabulary

ENCLOSURE D

**Exposure Quick Look Checklist**

<b>Data</b>	
<b>Category</b>	<b>Requirements to Achieve Objective</b>
Visible – CD&D	1. <a href="#">DDMS</a> information entered in an Enterprise Catalog 2. Data can be found by a Federated Search
Accessible – Policy	If your data is not accessible to all users you must present the user with written policy on how to gain access to the site within two clicks that is understandable by anticipated and unanticipated users
Accessible – Operational	NCES Federated Search results provide active link that when it is selected provides access to the website without requiring the user to enter credentials (i.e. username, password) or by exercising policy (e.g. request access, obtain login)
Understandable – User	The keywords entered in the DoD Discovery Metadata Specification ( <a href="#">DDMS</a> ) record in the Enterprise Catalog must reflect common terms used by the user <ul style="list-style-type: none"> <li>– Search terms/keywords appropriate for Mission area or data type</li> <li>– Described data understandable to both anticipated and unanticipated user</li> <li>– Mission data maps back to search terms</li> </ul>

<b>Service</b>	
<b>Category</b>	<b>Requirements to Achieve Objective</b>
Visible - MDR	WSDLs, XML Schema Definitions (XSDs), and XML instances will be registered in <a href="#">MDR</a>
Visible – UDDI	Operational end points registered in the NCES Services Registry ( <a href="#">UDDI</a> ) by referencing the WSDL in the <a href="#">MDR</a> (note: WSDL must first be registered in the <a href="#">MDR</a> )
Accessible – UDDI	1. NCES Services Registry ( <a href="#">UDDI</a> ) registered service end-points provide transparent machine-to-machine access to operational data at the targeted security enclave 2. NCES Services Registry ( <a href="#">UDDI</a> ) registered service links to accessible WSDL definition in the <a href="#">MDR</a>
Accessible – Policy	1. Service Provider has written policy registered in the DoD <a href="#">MDR</a> listing actions necessary to gain transparent machine-to-machine access to services 2. Policy information as well as the steps listed to request access to the service made clear for unanticipated developer
Understandable – MDR	Service provider schemas and supporting documentation registered in <a href="#">MDR</a>
Understandable – COI	Service schemas conform to standard (COI approved) vocabulary