

## The Mandate

On 23 Jan 2013, the Department of Defense (DoD) Chief Information Officer (CIO) issued a memo mandating the use of DoD Enterprise Directory Services (EDS) by all DoD Components.

## Background

EDS is a suite of products and services offered by the Defense Information Systems Agency (DISA) and the Defense Manpower Data Center (DMDC) that provides secure DoD enterprise identity and contact attributes. It is comprised of enterprise provisioning, directory, and synchronization services, and enterprise white pages.

## Why an IdSS Machine Interface (IdMI)?

The establishment of an IdMI connection with DISA provides a well-defined EDS interface with enterprise identity and contact information for DoD-level and Component-level IT directory systems. The identity and contact data includes person and persona elements, including Public Key Infrastructure (PKI) certificates, for personas that have a current DoD Common Access Card (CAC). Utilizing an IdMI connection helps DoD Components achieve compliance with the DoD EDS Memo.

## Obtain EDS Data in 3 Easy Steps with IdMI

### Step 1: Identification

- Choose from one of the IdMI delivery model options →

### Step 2: Documentation

- Document technical details in an IdMI Customer Interface Specification (CIS) document
  - Identify the selected model and frequency of data push/pull
  - Provide DISA Internet Protocol (IP) addresses for firewall changes
  - Identify any filters required
- Provide Privacy Impact Assessment (PIA) or System of Record Notice (SORN)
- Provide Authority to Operate (ATO)
- Sign Memorandum of Agreement (MOA)

### Step 3: Integration

- Establish IdMI connection and deploy to production environment

#### Model 1

##### DISA Push: Uses Forefront Identity Manager (FIM)

- DISA performs transformations, policy filtering, and change log tracking on behalf of the component
- Groomed data pushed to the customer's account
- Multiple available management agents allow DISA to supply most popular database, directory, or file systems

#### Model 2

##### Component Pull: Uses Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) (LDAP/S) Synchronization Engine

- Component uses qualified identity management solution that has change log functionality to pull data from IdMI based on a pre-established schedule
- Utilizes LDAP/S protocol

#### Model 3

##### Component Pull: Uses Structured Query Language (SQL) Synchronization Engine

- Component uses an SQL connection to better control the update
- Incremental update frequency and filtering of information can be done before the data is transmitted to the component

#### Model 4

##### Read Only Replica Model (Need based only)

- DISA writes IdSS data into an LDAP directory
- Component sets up corresponding LDAP server to read from and DISA replicates IdSS data to the server via IdMI
- Component consumes all 4.5 million objects (NIPRNet) from the DISA Enterprise Global Address List (GAL)

DISA Enterprise Services Directorate  
 IdAM EDS  
 Email: DISA.EDSMemo@mail.mil

For more information on IdMI, visit:  
<http://iase.disa.mil/idam/eds/idss.html>