



IMPLEMENTATION PLAN FOR ORGANIZATION UNIQUE IDENTIFICATION REGISTRY

Arlington, Virginia
July 6, 2007
Version # 27

Personnel and Readiness Information Management

Executive Summary

This plan addresses the overall high-level implementation requirements for the Organization Unique Identification (OID) Registry, to include program management and implementation actions. It also provides information on the background of the initiative, OID Registry standards and supporting technology, data requirements criteria, information security, infrastructure, and business process improvement issues related to the OID. The plan does not discuss or direct specific actions regarding the use of the organization information in business processes. DoD Directive (DoDD) 8320.03 *Unique Identification for a Net-Centric Department of Defense*, March 2007 and DoD Instruction (DoDI) 8260.03 *Organizational Force Structure Construct (OFSC) for Global Force Management (GFM)*, August 2006 provide the overarching guidance and direction for implementing the OID and the OID Registry technology.

The OID is a means of uniquely distinguishing one organization from another whenever organizational information is exchanged between systems on the Global Information Grid (GIG). The OID for an organization will be the equivalency of an Internet Protocol (IP) address for an email address. The OID will not replace existing identifiers, to include international and national accepted identifiers [e.g., Unit Identification Code (UIC), Personnel Accounting Symbol (PAS), Data Universal Numbering System (DUNS), or Commercial And Government Entity (CAGE)].

The DoD lacks a centralized repository for the OIDs or the organization identifiers in use today. Currently no specific authoritative data source (ADS) exists where DoD organizations can access Department-wide information. The OID Registry technology will leverage the GFM Data Initiative (DI) and will function as a central repository for OID information. It will be a single authoritative organizational identification source available to support all business and warfighting operations across the Department. It will also provide a mapping to current organization identifiers in use within internal business systems.

The scope of this OID Implementation Plan includes management, required implementation actions, data standards, information security, infrastructure, and business process improvement issues.

- Management:
 - The OID Registry and supporting technology will be developed and maintained in conjunction with the Office of the Secretary of Defense (OSD) Org Server. The OSD Org Server Implementation Plan (available separately) identifies the Office of the Under Secretary of Defense (OUSD) Personnel and Readiness (P&R) Readiness (R) as the sponsor for the OSD Org Server. As such, OUSD (P&R) (R) and Personnel and Readiness Information Management (P&R IM) will be responsible for the requirements, development and implementation of OID Registry technology.

- Implementation:
 - Initial Operating Capability (IOC) is scheduled for September 1, 2007, and will include a sample of unclassified representative DoD organizations. Full Operating Capability (FOC) for classified and unclassified environments will occur in October 2009 with GFM Org Servers FOC for all forces.
 - Implementation actions consisting of development, testing, training, funding, accreditation, and other specified actions are discussed in depth within Chapter 3.
 - Development will address eight specific actions beginning with determination of data element requirements and concluding with the achievement of FOC.
 - Testing on initial features will begin May 2007 and will be completed with the testing of the user interface processes in January 2008.
 - Training requirements and method identification will begin in March 2008, and will conclude with delivery of the sustainment package in October 2008.
 - Funding requirements are already being addressed and will be reviewed annually.
 - Accreditation began with requirements determination and will be completed in October 2008.
 - Other requirements will be addressed as required throughout the development process.

- Proposed Data Standards:
 - The OUID is constructed using the tenets of the Force Management Identifiers (FMIDS) technology used in GFM DI. As with the FMIDS, the OUID will be a unique and non-intelligent 64 bit number that can be displayed as 16 character hexadecimal or 20 digit numeric with a limit of 2^{64} (18,446,744,073,709,551,615) possible combinations.
 - OUID Registry technology will be implemented in accordance with DoD interoperability, security, and information assurance standards. The OUID will support GIG and Net-Centric data strategies.
 - The implementation of OUID Registry technology does not necessarily require supported system modification. Implementation options include creating an alternate key for the OUID in the system organization table, adding a crosswalk table between the internal identifier and the OUID, or using organization aliases to crosswalk to the OUID via the alias list maintained in the OUID Registry.

- Information Security:
 - The OUID Registry will include both an unclassified and a classified environment.

- Infrastructure:
 - OUID Registry technology will be built to address mandatory GFM requirements to support peacetime, wartime, and contingency requirements for the unique identification of organizations.

- Business Process Improvement:
 - The development of OUID Registry technology provides capabilities not previously available to DoD and establishes a single authoritative source for

- uniquely identifying organizations. These improvements can occur with potentially minimal impact on legacy systems.
- As OUID Registry technology does not address how the OUID is to be used in current or future DoD systems. It does not constrain ongoing DoD Business Process Improvement efforts – rather, it supports them. Additionally, current and future system program managers are now afforded the opportunity to reexamine and continuously refine their operations based upon use of OUID Registry technology.

TABLE OF CONTENTS

EXECUTIVE SUMMARY I

CHAPTER 1 – INTRODUCTION..... 1

 1.1 PURPOSE..... 1

 1.2. SCOPE..... 1

 1.3. BACKGROUND..... 1

CHAPTER 2 - OUID PROGRAM MANAGEMENT..... 2

 2.1. DoD OUID REGISTRY IMPLEMENTATION OFFICE (IO)..... 2

 2.1.1. *Interfaces with Other Functional Areas*..... 2

 2.2. INTEROPERABILITY 3

 2.3. REQUIREMENTS DETERMINATION 3

 2.3.1. *OUID Registry Architecture* 4

 2.3.2. *Investment Cost*..... 4

 2.3.3. *Operating Costs* 4

 2.4. FUNDING 5

 2.5. OTHER PROGRAM MANAGEMENT ISSUES 5

 2.5.1. *Logistics Support* 5

 2.5.2. *Training* 6

 2.5.3. *New Equipment Training* 6

 2.5.4. *Sustainability and Follow-On Training* 7

 2.5.5. *Safety*..... 7

CHAPTER 3 – IMPLEMENTATION ACTIONS 8

CHAPTER 4 – DOD OUID REGISTRY IMPLEMENTATION OFFICE (IO) 11

 4.1. AUTHORITY 11

 4.2. PURPOSE 11

 4.3. SCOPE 11

 4.4. MISSION..... 11

 4.5. ROLES AND RESPONSIBILITIES 11

APPENDIX A - PROPOSED DOD OUID STANDARDS 13

 A.1. UNIQUE IDENTIFICATION 13

 A.2. FORCE MANAGEMENT IDENTIFIERS (FMIDS)..... 13

 A.3. THE ORGANIZATION UNIQUE IDENTIFIER (OUID) 14

 A.4 OUID ATTRIBUTES, DATA ELEMENTS, DEFINITIONS, AND VALUES 15

APPENDIX B - INFORMATION SECURITY 16

 B.1. SYSTEM ACCESS MANAGEMENT AND WEB SERVICE SECURITY..... 17

 B.2. USER ACCESS..... 17

 B.3. EXCHANGE OF INFORMATION ACROSS DOMAINS 17

APPENDIX C – INFRASTRUCTURE 19

 C.1. GFM ORG SERVER/FMIDS SYSTEM AND OUID REGISTRY OVERVIEW 19

 C.2. ABNORMAL OPERATIONS 20

APPENDIX D - BUSINESS PROCESS IMPROVEMENT..... 21

 D.1. USING OUID REGISTRY TECHNOLOGY TO IMPROVE BUSINESS PROCESSES 21

 D.2. OTHER CONSIDERATIONS..... 21

APPENDIX F – ACRONYMS AND GLOSSARY 23

APPENDIX G – REFERENCES..... 31

Chapter 1 – Introduction

1.1 Purpose

The OUID Registry Implementation Plan is a living document that supports the OUID in accordance with DoDD 8320.03, *Unique Identification for a Net-Centric Department of Defense*, March 2007. The OUID Registry also supports DoDI 8260.03, *Organizational and Force Structure Construct (OFSC) for Global Force Management (GFM)*, August 2006, and GFM unique identification requirements. Additionally this plan identifies lead and supporting organizations and programs, describes necessary actions, and assigns completion dates.

1.2. Scope

This plan supports the Services, Joint Staff, and OSD use of the OUID to uniquely and unambiguously identify organizations. It addresses the overall high-level implementation requirements for the OUID Registry, to include program management and implementation actions. The appendices address the background, OUID Registry standards and supporting technology, data requirements criteria, information security, infrastructure, and business process improvement. This plan does not discuss or direct specific actions regarding the use of the organization information in business processes (e.g., it discusses how to obtain organization information for use in such processes as financial transactions, but does not discuss how the organization information will be used in financial transactions).

Additionally, this plan identifies issues that need to be resolved, identifies implementation actions, and assigns responsibilities. Further information can be found in the OUID Registry Concept of Operations (ConOps).

1.3. Background

OUSD (P&R) (R) began work on determining the need, requirements, and processes for implementation of OUID Registry technology in March 2005. Since that time, research has been conducted into current organization identification processes and identifiers utilized by the DoD. Additionally, research and analysis has been conducted regarding the actual needs of DoD organizations and processes for organization identification. This work included determining requirements through a series of working groups attended by all Services, the Joint Staff, and multiple OSD offices. Requirements were also leveraged from concurrent efforts, such as the Standard Financial Information Structure (SFIS) and Enterprise Resource Planning (ERP) system development. The OUID ConOps is available as a separate document.

Chapter 2 - OUID Program Management

The DoD OUID effort requires effective management in order to implement this plan by FY 08. Joint Staff J-8 (MASO) is designated as the Sponsor for the Global Force Management Data Initiative (GFM DI) and is responsible for all common documentation, periodic reporting, and funding requirements determination required to support GFM DI capabilities development and acquisition processes. In support of this effort, the OUSD (P&R) (R) Defense Readiness Reporting System (DRRS) Implementation Office (DIO) has been designated as the OSD Org Server Program Management Office (PMO). OUSD (P&R IM) has been designated as the OSD Org Server Implementation Office (IO) supporting the OSD Org Server PMO. The OUID Registry and supporting technology and information will be developed and maintained as a part of the OSD Org Server. As such, OUSD (P&R) (R) and P&R IM will be responsible for the development and implementation of OUID Registry technology. P&R IM will be designated as the OUID Implementation Office (IO). This chapter discusses program management actions and issues.

2.1. DoD OUID Registry Implementation Office (IO)

The OUID Registry IO has concentrated its initial efforts as Chair of the DoD OUID Working Group. The OUID Working Group efforts have focused on planning, requirements determination, and initial OUID Registry development actions. Additionally, the office has worked directly with other DoD Business Transformation efforts, such as the Standard Financial Information Structure effort, to further define requirements and implementation actions. Work has also included close interaction with the GFM DI, such as force structure determination and supporting Org Server technology capabilities.

The office has assumed full responsibility for its mission to promote, manage, coordinate, and document the application of DoD OUID Registry technology, doctrine, and processes in support of warfighters and DoD business processes. The office's scope, mission, roles, responsibilities, and relationships with other DoD activities are described in Chapter 4.

2.1.1. Interfaces with Other Functional Areas

OUID Registry technology provides for unique identification of organizations across a wide spectrum of functional areas. The OUID Registry IO has, and will continue to, coordinate with other functional areas to support initiatives such as Financial Enterprise Resource Planning program development, implementation of other DoD unique identifiers (e.g., Real Property and Site unique identifiers), DRRS development, or GIG-related efforts.

2.2. Interoperability

Automated Information System (AIS) to AIS interfaces for sending or receiving data provide interoperability. The OUID ConOps recognizes a direct interface between systems as the preferred method of transferring data. Although attaining this interoperability through implementation of GIG concepts and Net-Centric Enterprise Services (NCES) is the goal, DoD has an immediate need for the data that OUID Registry technology can provide. OUID Registry technology will be developed to take advantage of current and future interoperability services. To that end, OUID Registry processes have been developed to support legacy system usage of the OUID and to provide for incorporation of OUID information into developing any future systems. The ability to transition to usage of the GFM DI Org Servers and their data exchange capabilities has also been included in OUID Registry processes.

The implementation of OUIDs across the DoD enterprise will be in accordance with the system processes as outlined in applicable DoD directives and system technical direction. All new systems requiring organization information will be developed with the capability to use OUIDs within that system and to use the OUID when interfacing with other systems. This will provide the framework for migration to the use of one organization identifier across DoD for information discovery and sharing in a Net-Centric environment.

Interoperability directions as outlined in DoDD 8320.2, *Data Sharing in a Net-Centric Department of Defense*, ASD (NII)/DoD CIO, December 2, 2004, have been followed in the development of the processes required for the OUID and are outlined in the OUID ConOps.

2.3. Requirements determination

The technology supporting the OUID Registry is dependent upon the technology developed for the GFM Org Servers. Specifically, the OUID leverages the ideas developed to support FMIDS creation and usage, along with the functionality required to support exchange of OUID information with user systems.

The major challenges in identifying requirements are:

- Determining macro requirements for implementation and use of the OUID Registry;
- Forecasting investment cost to acquire and install the technology;
- Identifying preferred implementation and usage processes as well as necessary modifications of the technology to support implementation processes;
- Establishing operating cost to maintain, operate, and upgrade OUID Registry technology.

These challenges are addressed in the following subsections.

2.3.1. OUID Registry Architecture

The information technology for the GFM Org Servers, especially the technology required for creation and management of FMIDS, provides the fundamental architecture for the OUID. Further architecture requirements are associated with the OUID Registry which will serve as the means of registering the OUID and associated organization information. In June 2006, the Joint Staff requested that the Services, Joint Staff, and OSD (P&R) identify the architecture and funding required to develop and sustain the GFM Org Servers. OUID architecture and funding requirements will be included in that effort.

As with the OSD Org Server, versions of the OUID Registry will support the unclassified and classified environment(s). Any additional costs and facilities will be addressed with those of the OSD Org Server. The classified Registry will include the unclassified data as well as the classified data. Both versions will be replicated to ensure the availability of data and services.

Resources will not be provided to meet OUID Registry technology implementation requirements in user systems.

2.3.2. Investment Cost

The investment cost is not merely determined by identifying the OUID Registry technology to be purchased. It requires identifying the total cost associated with fielding the system and must include the costs associated with the Level of Effort (LOE) required to field the technology. Cost elements include the following:

- Hardware for primary and back up sites
- Software and firmware for primary and back up sites
- Modifications of AIS software to accept OUID data and support amended business processes
- Site preparation
- Installation
- Training
- Travel and per diem

2.3.3. Operating Costs

Operating costs are a large component of the total requirement and will be addressed by OSD in their Program Objective Memorandum (POM) submissions. A determination by P&R (Readiness) will be made as to whether these costs can be captured in the GFM Org Server POM submissions. The costs consist of maintaining and upgrading the hardware, software, infrastructure, and operator proficiency as well as providing telecommunications, systems administration, and program management.

2.4. Funding

Table 2-1: OUID Funding by Fiscal Year

FY08	FY09	FY10	FY11	FY12	FY13
2.0	2.1	2.2	2.3	2.4	2.5

* values are in millions of dollars.

Issue: OUID Registry technology requirements need to be addressed routinely during the DoD Planning, Programming, Budgeting, and Execution (PPBE) cycle.

To support addressing OUID Registry technology requirements, the following actions must be completed:

- **Action 1:** Reflect the importance of OUID Registry technology in Integrated Priority Lists to the Joint Staff.
- **Action 2:** Reflect the importance of OUID Registry technology in DoD Directives, Instructions, and Planning Guidance.
- **Action 3:** Ensure DoD Component planners and programmers are fully aware of the importance and use of OUID Registry technology in DoD processes and the requirement to fund.
- **Action 4:** Coordinate OUID Registry technology funding with GFM Org Server Executive Agent and DoD Component Org Server management.

2.5. Other Program Management Issues

The remaining program management issues concern logistics support, training, and safety.

2.5.1. Logistics Support

Joint Staff J-8 (MASO) is designated as the Sponsor for the GFM DI and is responsible for all common documentation, periodic reporting, and funding requirements determination required to support GFM DI capabilities development and acquisition processes. In support of this effort, OUSD (P&R (R) DIO has been designated as the OSD Org Server PMO. The DIO will serve as the logistics support organization for OUID Registry technology.

A major component of logistics support is maintenance, which is performed at two levels.

- **Operator-organizational maintenance:** Units and activities perform maintenance in accordance with warranty guidelines and manufacturer's manuals

- Contractor maintenance: Hardware, software, and firmware warranty service and maintenance beyond a user's capability

Requirements will need to be identified surrounding security of information and maintenance procedures.

Issue: Logistics support will need to be evaluated by users after an initial period of operation.

2.5.2. Training

The introduction of a significantly different way of identifying organizations and utilizing the information available in the OUID Registry will succeed only if users and administrators of the OUID Registry are knowledgeable and competent in their roles and responsibilities. Consequently, a comprehensive OUID Registry training program that integrates all forms of training is essential. Most OUID Registry use is associated with system-to-system data exchange. These data exchange processes require proper interface set-up and maintenance to and from Authoritative Data Sources and user systems. Additionally, OUID Registry system administrators require the skills necessary to set up and manage the OUID Registry and associated processes such as user account management. Training associated with OUID Registry technology will be addressed within the context of GFM Org Server training with emphasis on the unique processes associated with the OUID Registry. Personnel receiving training must possess the basic software and hardware skills needed to support OUID Registry technology processes.

2.5.3. New Equipment Training

New equipment training must address the following obstacles to ensure training effectiveness:

- Training occurring too far in advance of implementation
- Training of system administrators, but not of supervisors or operators
- Excessive reliance on demonstrations rather than application of OUID Registry technology (especially important for interface set-up and maintenance training)
- Lack of documentation of OUID Registry technology software changes
- No written instructions on proposed business process changes

Training must be presented in the context of business processes and supported systems. New equipment training should be provided by the PMO with assistance from OUID Registry technology developers.

2.5.4. Sustainability and Follow-On Training

Attrition and personnel rotations make sustainability training important to the continued effective use of OUID Registry technology. Sustainability training must actively be in place in order to ensure that newly assigned personnel remain aware of the OUID Registry processes and incorporate that knowledge and skill development into appropriate training programs. OUID Registry technology training requirements should be incorporated into site (ADS and user system) qualification programs.

OUID Registry system administrator and operator training and qualification procedures, if appropriate, will be included in GFM Org Server administration and operation training. New training required due to refinement of the OUID Registry processes and software will be developed and pushed to ADS and User System points of contact (POCs) with instructions for revision of previous training materials.

2.5.5. Safety

Human System Integration and safety, to include standard electronic safety procedures, will be developed, published, and implemented based upon OUID Registry fielding decisions including, but not limited to, installation facilities, hardware, graphical user interface design, maintenance requirements, and determination of abnormal operating conditions and risks.

Chapter 3 – Implementation Actions

This plan directs integration of OUID Registry into DoD processes to facilitate unique identification of organizations. The following table (Table 3-1) identifies the actions, identifies lead and coordinating organizations, and assigns completion dates. Actions are grouped into subject areas (e.g., OUID Registry Development, Training, and Interface), designated by a subject area and sequence number (e.g., D-1, Development Action 1). Each completion date is set to a Fiscal Year quarter (e.g., 01FY07 refers to first quarter, Fiscal Year 2007). Completion dates are relative to the Functional Area number and are not in chronological sequence.

Table 3-1: OUID Implementation Actions

Functional Area	No.	Action	Lead Organization	Coordinating Organizations	Planned Completion Date
Development	D-1	Determine OUID Registry Data Element Requirements	OUSD (P&R)(R), OUSD (P&R) P&R IM	Services, OSD, Enterprise Resource Planning Organizations	Completed: 04FY2006
	D-2	Determine OUID Business Process Requirements	OUSD (P&R) P&R IM	Services, OSD, Enterprise Resource Planning Organizations	Completed: 02FY2007
	D-3	Create OUID Registry	OUSD (P&R)(R)	OUSD (P&R) P&R IM	04FY2007
	D-4	Complete features required for OUID Registry IOC	OUSD (P&R)(R)	OUSD (P&R) P&R IM	04FY2007
	D-5	Prepare the system for production use by selected ERP Programs	OUSD (P&R)(R)	OUSD (P&R) P&R IM, ERP Programs	02FY2008
	D-6	Incorporate ADS Interface Capability	OUSD (P&R)(R)	OUSD (P&R) P&R IM, ADS	02FY2008
	D-7	Populate OUID Registry with Initial Set of OUIDs and associated information from Component Org Servers	OUSD (P&R)(R)	OUSD (P&R) P&R IM, ADS	04FY2007
	D-8	Complete features and data base population required for OUID Registry FOC	OUSD (P&R)(R)	OUSD (P&R) P&R IM, Services, OSD, Enterprise Resource Planning Organizations	01FY2008
Testing	T-1	Complete testing of initial features	OUSD (P&R)(R)	OUSD (P&R) P&R IM	02FY2008
	T-2	Complete testing of ADS interface processes	OUSD (P&R)(R)	OUSD (P&R) P&R IM, ADS (Services, JS, OSD)	03FY2008
	T-3	Complete testing of user system interface processes	OUSD (P&R)(R)	OUSD (P&R) P&R IM, ERP (Services)	03FY2008

Functional Area	No.	Action	Lead Organization	Coordinating Organizations	Planned Completion Date
	T-4	Complete testing of user interface processes	OUSD (P&R)(R)	OUSD (P&R) P&R IM, ERP, Services, JS	03FY2008
Training	Tr-1	Determine initial and sustainability training requirements and methods	OUSD (P&R) P&R IM, OUSD (P&R)(R)	Services, OSD, Enterprise Resource Planning Organizations	03FY2008
	Tr-2	Complete initial training	OUSD (P&R) P&R IM, OUSD (P&R)(R)	Services, OSD, Enterprise Resource Planning Organizations	04FY2008
	Tr-3	Develop and deliver sustainability training package	OUSD (P&R) P&R IM, OUSD (P&R)(R)	Services, OSD, Enterprise Resource Planning Organizations	04FY2008
Funding	F-1	Determine and provide funding for development	OUSD (P&R)(R)	OUSD (P&R) P&R IM	02FY2007
	F-2	Determine and provide funding for implementation	OUSD (P&R)(R), Services, OSD, Enterprise Resource Planning Organizations	OUSD (P&R) P&R IM	04FY2007
	F-3	Determine and program for OSD Org Server technology operational costs	Services, OSD, Enterprise Resource Planning Organizations	OUSD (P&R) P&R IM	Annual
Accreditation	A-1	Determine accreditation requirements	OUSD (P&R), OUSD (P&R) P&R IM	ASD/NII	03FY2008
	A-2	Complete accreditation	OUSD (P&R)(R), OUSD (P&R) P&R IM	ASD/NII	04FY2008
Other	O-1	Designate OUID Sponsor	OUSD (P&R)		01FY2008
	O-2	Establish OUID Implementation Office	OUID EA	OUSD (P&R)	01FY2008
	O-3	Complete policy and acquisition documentation	OUSD (P&R), OUSD (P&R) P&R IM	Services, OSD, Enterprise Resource Planning Organizations, ASD/NII	
	O-4	Determine organization to manage OUID operations	OUSD (P&R)(R)		01FY2008
	O-5	Develop, test, and certify OUID cross domain solution	OUSD (P&R)(R)	TBD	04FY2008
	O-6	Maintain and Update OUID standards	OUSD (P&R)(R), InnovaSystems, OUSD (P&R) P&R IM	Services, OSD, ASD/NII	Ongoing

Functional Area	No.	Action	Lead Organization	Coordinating Organizations	Planned Completion Date
	O-7	Establish and conduct OUID Registry Panel meetings	OUSD (P&R)(R)	Services, OSD, ASD/NII	Ongoing

Chapter 4 – DoD OUID Registry Implementation Office (IO)

This section describes the DoD OUID IO's scope, mission, roles, responsibilities, and relationships with other DoD activities.

4.1. Authority

OUSD (P&R) (R) DIO has been designated as the OSD Org Server PMO with OUSD (P&R IM) designated as the OSD Org Server Implementation Office (IO) supporting the OSD Org Server PMO. The OUID Registry and supporting technology and information will be developed and maintained as a part of the OSD Org Server. OUSD (P&R IM) is responsible for requirements gathering which will enable OUID development. OUSD (P&R) (R) will be responsible for the development and implementation of OUID Registry technology based on the requirements analysis performed by P&R IM.

4.2. Purpose

This document is the basis of the DoD OUID Registry IO's concept of operation and documents the scope, mission, roles and responsibilities, and relationships of the OUID Registry Implementation Office with other DoD activities.

4.3. Scope

The DoD OUID Registry IO will operate with guidance provided by OUSD (P&R) (R) and administrative support provided by OUSD (P&R IM).

4.4. Mission

The DoD OUID Registry IO will provide determination of requirements, program management, implementation coordination, and documentation development to promote the development and implementation of the OUID Registry, and allow OUIDs to be utilized throughout the DoD.

4.5. Roles and Responsibilities

Working with the DUSD (P&R) (R), the DoD OUID Registry IO will ensure that the Department's requirements for unique identification of organizations are determined. Additionally, the office will oversee the development and implementation of required OUID Registry technology. The immediate focus will be on development of the initial OUID Registry technology and testing of the technology. The office will serve as the proponent for promoting knowledge and use of OUID Registry technology. It will assist the Services, OSD Offices, Defense Agencies, and Defense Field Activities as necessary to ensure that OUID Registry policies, processes, and procedures are fully integrated and

institutionalized. It will ensure that OUID Registry standards are developed, documented, enforced, and revised as necessary, to meet DoD requirements. Specific responsibilities of the OUID Registry IO include:

- Perform program management responsibilities as outlined in the OUID Registry Implementation Plan
- Work with the Services, OSD Offices, Defense Agencies, and Defense Field Activities to implement the use of the OUID Registry to support the uniquely identification of organizations
- Provide OUID Registry standards and management of standards revision
- Establish metrics for evaluation of OUID Registry technology
- Oversee testing of OUID Registry technology and incorporate required changes into OUID Registry documentation and technology development
- Chair the OUID Registry ADS Panel

Appendix A - Proposed DoD OUID Standards

A.1. Unique Identification

An identifier is a property or value that allows differentiation between one or more objects or entities. Computers tag all data with an identifier and use it to classify and store data.

To ensure that organization data does not collide with other data, development of an enterprise-wide unique identification schema is necessary. Although any schema could be chosen, the basic requirements for the identifier are:

- A single attribute with no embedded intelligence
- Identical size and form across all identifiers
- A size chosen to be as small as possible.

The reason for these characteristics is that in a Net-Centric environment, users do not know what systems will be using their data. It is preferable to implement the OUID according to the above guidelines and avoid the pitfalls of the past, including:

- As soon as one embeds intelligence into an identifier, it severely limits its usefulness. Vehicle Identification Numbers (VIN), Social Security Numbers (SSN), and even telephone numbers, are examples of identifiers with embedded intelligence, for which the systems underwent massive (and expensive) changes.
- Making all of the identifiers the same size and form will help build and maintain functionality. If software developers know the specification for a given field they can integrate information more rapidly.
- The identifier has to be unique across all systems of the enterprise – to include the tactical (i.e., low-bandwidth) systems. Low-bandwidth systems will slow or fail using identifiers that are too cumbersome.

Enterprise-wide identifiers uniquely identify data across the entire enterprise, not just within a specific table, function, or type of database. Since organization data will be used by multiple systems, functions, and databases, it is critical that it use enterprise-wide identifiers.

A.2. Force Management Identifiers (FMIDS)

DoD Instruction 8260.03, *Organizational and Force Structure Construct (OFSC) for Global Force Management (GFM)*, dated August 23, 2006, requires that all force structure representation come from the DoD Component ADS (i.e., the Organization Server). The values for these representations are known as FMIDS.

FMIDS are the set of enterprise-wide unique identifiers that unambiguously tag all of the data within the GFMIEDM. The GFMIEDM currently contains 46 different tables (many of them imported directly from the 241 tables of the Joint Consultation Command and Control Information Exchange Data Model [JC3IEDM]) and each of those tables, and the data elements within those tables, has an identifier. These identifiers are known collectively as FMIDS.

FMIDS is the collective name for all the force structure information identifiers present in the Org Servers. Currently, the names used to identify force structure elements (units, positions titles, etc.) frequently differ among information systems. With FMIDS, systems will consistently reference elements of the force structure, such as organizations and command relationships, thereby facilitating interaction and integration. FMIDS are:

- A known size and format
- Unique across the enterprise
- Non-intelligent

To date, identification is a task that every system in DoD has grappled with, and each has addressed it in its own way. In the Net-Centric environment, however, DoD is not simply passing around files; rather, the enterprise is sharing and integrating data.

In the end, each user will benefit from ensuring the unique identification of data. When returning to a system to refresh outdated data, one will need to identify exactly where that data came from to ensure uniformity. Users must be able to uniquely track data to and from the source or face “computer chaos.”

FMIDS uniquely tag each force structure data element across the enterprise with one non-reusable identifier, and each identifier will be assigned to only one force structure element. FMIDS contain no information about the element they describe; rather, they are simply identifiers that distinguish elements across the enterprise. FMIDS uniquely identify GFMIEDM components within the OFSC. Each piece of information that a system or application pulls from an Org Server will be associated with a unique FMIDS that will identify it throughout the enterprise.

FMIDS are a 64-bit number (binary) that can be displayed as a 16-digit hexadecimal number or 20-digit numeric up to the value of 2^{64} (18,446,744,073,709,600,000) if required. However, the primary use for FMIDS is automated system-to-system data exchange.

A.3. The Organization Unique Identifier (OUID)

One of the tables within the GFMIEDM is known as the Organization table, and is used to identify all organizations. This table consolidates organizations and their associated FMIDS. The subset of FMIDS is known as the OUID.

Within the GFMIEDM, an organization is created to serve as an aggregation point for other entities; therefore, it may be categorized based upon the reason for its creation. To date, five categories have been defined:

- Billet Organization
- Crew Organization
- Doctrinal Organization
- Garrison Organization
- Work Load Equivalent Organization

As currently defined, OUIDs uniquely identify doctrinal organizations generated by the Org Servers; but if a need is identified, it can be expanded to support the other organization types above (e.g., billet). Since the OUID uniquely identifies a specific organization, it also has all of the attributes (from the GFMIEDM table) of that organization that are contained in the Org Server, such as the formal name, derived names, and nicknames. Additionally, the OUID Registry has the capability for alias information (i.e., alternative ways systems currently reference those units) to be associated with the OUID. The OUID is the minimum requirement for force structure information.

A.4 OUID Attributes, Data Elements, Definitions, and Values

Specific OUID attributes, data elements, definitions, and values are detailed in Appendices to the OUID Registry ConOps.

Appendix B - Information Security

OUID Registry technology will provide the capability to more efficiently and effectively capture and exchange organization information across the Department. It will allow for fast and accurate Net-Centric data exchange, and foster the ability to process and integrate information, including classified and “sensitive but unclassified” information, through a myriad of methods across differing situations. To protect OUID information and network domains, OUID Registry technology will incorporate all appropriate physical and logical data security measures in accordance with DoD policy. Information Assurance (IA), network domain and cross domain certification, and authorization and accreditation procedures will be followed. Access to OUID information will also be based upon specific roles and permissions and a defined access approval process.

The OUID Registry will include unclassified and classified environments. The Registry’s IA Mission Assurance Category (MAC) will be MAC III for both environments. The MAC III designation identifies IA integrity and availability controls for systems that are necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. All MAC III access, security, and reliability requirements will be met.

Additionally, the IA Confidentiality Level of the unclassified OUID Registry will be “Sensitive.” The “Sensitive” designation identifies systems which process unclassified information not cleared for public release. The classified OUID Registry will have an IA Confidentiality Level of “Classified,” which identifies a system which processes classified information.

All OUID Registry system certification, authorization, and accreditation requirements for both classified and unclassified environments will be met prior to the system Initial Operating Capability (IOC) date of September 2007.

A System Security Authorization Agreement (SSAA) will be prepared by the developer. The SSAA is the baseline document used in the certification, authorization, and accreditation process. The OUID Registry SSAA will identify the system, system security, and operational requirements; identify security risks and risk management actions; identify required resources, roles and responsibilities; and identify the level of effort (costs, manpower, training, etc.). Certification, authorization, and accreditation processes and compliance requirements that must be completed during OUID Registry development include the:

- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- Global Information Grid (GIG) Interconnection Approval Process (GIAP)
- Secret and Below Interoperability (SABI) Accreditation
- Networks and Information Integration (NII) Information Assurance Checklist.

B.1. System Access Management and Web Service Security

The OUID Registry will use the Simple Object Access Protocol (SOAP) for internet communications. SOAP is an Extensible Markup Language (XML) based protocol which provides a standardized, platform/language-independent data exchange mechanism. It will enable Registry data to be sent across any communication channel, including web services and Simple Mail Transfer Protocol (SMTP) messaging.

Web Service (WS) Security will also be used to enhance the security of OUID Registry SOAP messaging. WS-Security addresses the security limitations of standard web services by enhancing SOAP messaging integrity, message confidentiality, and single message authentication. The WS-Security model allows for the development of scalable applications by providing the means for effectively communicating security credentials, by providing a mechanism for issuing lightweight, XML based tokens, and by providing the means for digitally signing SOAP messages.

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) cryptographic capability will be used to secure and encrypt the network layer when accessing the unclassified or classified OUID Registry web sites or web services. HTTPS provides secure communications by establishing a secured connection, and enforcing the exchange of certificates issued by a trusted Certificate Authority (CA). This SOAP-over-HTTPS approach will allow for the creation of a very secure OUID Registry environment by ensuring that communications are only with a known source, and by only sending encrypted data across the network layer.

B.2. User Access

User access will be based upon separately defined roles and permissions for the classified and unclassified OUID Registry environments. User access will comply with DoD IA Net-Centric/network domain security standards and practices, including Public Key Infrastructure (PKI). The OUID Registry, consistent with required security protocols and defined roles/permissions, will allow standard user access using either Common Access Card (CAC) and login, or Personal Identification Number (PIN) and password.

B.3. Exchange of Information Across Domains

A cross domain solution (CDS) device will be used to provide for the secure exchange information between unclassified and classified OUID Registry servers and associated security domains/networks. A CDS is a “guard” which allows the controlled sharing of information across security boundaries, prevents the unwanted flow of restricted data from a higher to a lower security domain/level, and protects the integrity of the higher security domain system or network from intrusion by viruses, etc.

The CDS will allow for the “push” of unclassified data to the secret-level classified Registry server either internally from the unclassified Registry server or externally

between the Non-Classified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET). Registry data updates will flow only one way, from the unclassified to the classified domain. OUID Registry responses to user requests for registry information will not flow across domains.

All required CDS documentation will be completed and approvals obtained prior to CDS connection to the SIPRNET.

Appendix C – Infrastructure

This chapter identifies the objective OUID Registry infrastructure to meet DoD OUID requirements. The GFM Org Server, FMIDS, and the OUID Registry are the only mandatory requirements with a goal of full integration by October 1, 2009, in concert with the GFM DI timeline. Implementation of the OUID Registry in other DoD systems (hardware and software) does not mandate use of additional infrastructure. The following sections describe capabilities to support routine and abnormal operations.

C.1. GFM Org Server/FMIDS System and OUID Registry Overview

The GFM Org Server will provide the ability to automatically disseminate authorized Force Structure information to any/all approved applications via web services.

The Org Server will be a centralized web-enabled application. There will be separate servers for FMIDS Seed prefixes (the FMIDS Seed Server), FMIDS (the FMIDS Server), and authorized organization and force structure constructs (the Org Server). OUID information will be maintained in the OUID Registry. The OUID Registry software may reside on the same hardware platform as one of the Org Servers or the FMIDS Server or reside on a separate hardware platform; final determination has not yet been made. Regardless, the OUID Registry will implement services and procedures similar to those in GFM Org/FMIDS Servers whenever possible.

The GFM Org Server Cluster will include database and web application modules. Access from outside users will be accomplished through HTTPS/SOAP processes. A firewall will exist between the GFM Org Server Cluster and outside users.

The servers will support a Services-Oriented Architecture by publishing web services that allow consuming applications to programmatically access the server. These services will be published as identified to solve a customer need. The Web Services support an XML format. This XML format will be similar to a subset of the GFMIEDM XML schema with extensions for OUID Registry unique requirements.

The network of GFM Org Servers will be deployed to both the unclassified and classified environments. OUID Registries will exist for both environments. OUID Registry services will be duplicated in the classified environment.

Web Services are not the only way that communications may occur. Transition of data from the unclassified network to the classified network will not be able to use Web Services, so SMTP based communication would be more appropriate.

FMIDS Seed Servers and FMIDS Servers and associated services will be duplicated in both environments. OUID Registry services will also be duplicated in the classified environment.

Web Service Enhancements (WSE) 2.0 will be used for routing and security where possible. In cases where this may not be possible, Secure Socket Layer (SSL) or Internet Protocol (IP) SSL/IP locking will be used for initial implementation of secure Web Services, migrating to a more robust PKI based solution.

WSE is a product that extends Web Services by providing implementation of additional Web Services protocols, including WS-Security for addressing message level security and WS-Addressing for managing content routing based on message content.

C.2. Abnormal Operations

The GFM Org Server redundancy processes and procedures will be leveraged to ensure continued operations in the case of loss of use of the primary OUID Registry.

All servers will be deployed in a clustered environment in order to guarantee availability in case of a single node failure. In addition, the cluster will be replicated across different sites in case of site failure.

Appendix D - Business Process Improvement

A principal recommendation of the OUID Registry ConOps is to improve DoD business processes through implementation of unique identification of organizations without the requirement to implement multiple identifiers across multiple systems, removal of various types of embedded information from current identifiers, or direct the change in use of current system generated identifiers.

A key factor in OUID Registry implementation, and the business process re-engineering surrounding its use, is that users of the OUID Registry identify these business processes. The OUID Registry does not drive change, it supports it. As an example, a group of systems currently utilize multiple identifiers at different stages in the allocation, disbursement, and accounting of fund expenditures. These systems can now use the OUID Registry and tie organizations relationally to the business process implemented to ensure the proper flow and accounting of expenditures without having to include multiple identifiers. The process to accomplish the transactions is defined by the financial community, not constrained by the OUID Registry. The following sections identify findings concerning business process improvement related to implementation of OUID Registry technology.

D.1. Using OUID Registry Technology to Improve Business Processes

Improvement of business processes must be a major consideration in determination of hardware, software, and information exchange capabilities. The ability to maintain the granularity and validity of information, along with efficient update and exchange intervals and speeds, is vital. The systems requiring the OUID Registry to conduct operations must be able to get the information they need when they need it. Even if the process is streamlined and effective, if it is not efficient, it is unsatisfactory.

The business process improvements associated with the development and implementation of the GFM Org Servers must be considered in implementation of OUID Registry technology. All efforts must be taken to ensure that OUID Registry technology is fully compatible with GFM DI technology. Additionally, the business process improvement technologies supporting the Department's business transformation along with warfighter system improvement and information exchange services must be considered to ensure OUID Registry technology compatibility and usability across the GIG.

D.2. Other Considerations

The success of the implementation of OUID Registry technology will ultimately be determined by the users of the OUID Registry and associated information. It is imperative that the business process improvement needs of ongoing, and future, transformation efforts be considered fully in the implementation, and improvement of, OUID Registry technology. In order to ensure user acceptance, OUID Registry technology data accessibility and accuracy must remain a top priority.

New and refined business processes associated with data transfer must be coordinated with GIG implementation and providers of information to the OUID Registry to ensure that providers, and users, of data approve of the procedures put in place to transfer and protect their data.

Appendix F – Acronyms and Glossary

Figure 1: Acronyms

Acronym	Definition
ADS	Authoritative Data Source
AIS	Automated Information System
ASD (NII)	Networks and Information Integration
BPN	Business Partner Number
C2IEDM	Command & Control Information Exchange Data Model
CA	Certificate Authority
CAC	Common Access Card
CAGE	Commercial And Government Entity
CCR	Centralized Contractor Registry
CDS	Cross Domain Solution
CM	Configuration Management
ConOps	Concept of Operations
DIACAP	DoD Information Assurance Certification and Accreditation
DLA	Defense Logistics Agency
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DRRS	Defense Readiness Reporting System
DUNS	Data Universal Numbering System
DUNS+4	Data Universal Numbering System + 4
ERP	Enterprise Resource Planning
ES	EwID Server
ESS	EwID Seed Server
EwID	Enterprise-wide Identifier
FedReg	Federal Agency Registration system
FMIDS	Force Management Identifiers
FOC	Full Operating Capability
FSS	FMIDS Seed Server
GFM	Global Force Management
GFM DI	Global Force Management Data Initiative
GFMIEDM	Global Force Management Information Exchange Data Model
GIAP	Global Information Grid (GIG) Interconnection Approval Process
GIG	Global Information Grid
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IA	Information Assurance
IO	Implementation Office
IOC	Initial Operating Capability
IP	Internet Protocol

Acronym	Definition
JC3IEDM	Joint Consultation Command and Control Information Exchange Data Model
LOE	Level of Effort
MAC	Mission Assurance Category
NATO	North Atlantic Treaty Organization
NCES	Net-Centric Enterprise Services
NII	Networks and Information Integration
OFSC	Organization and Force Structure Construct
Org	Organization
Org Server	Organization Server
OSD	Office of the Secretary of Defense
OUID	Organization Unique Identifier
OUSD (P&R)	Office of the Under Secretary of Defense for Personnel & Readiness
OUSD (P&R) (R)	Office of the Under Secretary of Defense for Personnel & Readiness (Readiness)
P&R IM	Personnel and Readiness Information Management
PKI	Public Key Infrastructure
PMO	Program Management Office
POC	Point of Contact
POM	Program Objective Memorandum
SABI	Secret and Below Interoperability
SAS	Seed Allocation Service
SSAA	System Security Authorization Agreement
SFIS	Standard Financial Information Structure
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
SSL/IP	Secure Socket Layer /Internet Protocol
SSN	Social Security Number
SOAP	Simple Object Access Protocol
URL	Uniform Resource Locator
USD (AT&L)	Office of the Under Secretary of Defense Acquisition Technology and Logistics
VIN	Vehicle Identification Numbers
WS	Web Service
WSE	Web Service Enhancements
XML	eXtensible Markup Language

Figure 2: Glossary

Term	Definition Source	Definition
Allocation	Forces For <u>Unified Commands FY2004</u>	Those forces and resources provided by the President or Secretary of Defense for execution, planning, or actual implementation. The allocation of forces is accomplished through procedures established for crisis action planning.
Authoritative Data Source (ADS)	DoDD 8320.2, Section E1.1.1. (provided by ASD NII)	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)."
Authorized Force Structure	GFM DI	Congressionally approved and funded organizations, units, personnel, and equipment that comprise the Department of Defense.
Billet or Position	DoDI 7730.64	Programmed manpower structure space typically defined by grade and occupation and associated with a specific unit or organization. A billet or position may be funded (authorized) or unfunded (generally called an unfunded requirement) and equates to 1 year of full-time support.
Certification	CJCSI 3137.01C	A statement of adequacy provided by a responsible agency for a specific area of concern in support of the validation process.
Classified Environment	GFM DI	Computer and networking systems (collectively referred to as Automated Information Systems (AISs) used to capture, create, store, process or distribute classified information that must be operated so that the information is protected against unauthorized disclosure or modification. Accreditation is required for an AIS to process classified information in an operational environment. The accreditation is based on documentation, analysis, and evaluation of AIS operations with respect to security risks and also on the safeguards associated with operation of the AIS.
Concept of Operations (ConOps)	CJCSI 3170.01	A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations. ConOps frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. ConOps is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Also called commander's concept.
Data	JP 1-02, Reference A	Representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

Term	Definition Source	Definition
Defense Readiness Reporting System (DRRS) Organization Server (Previously titled DoD Org Server)	GFM DI	The Organization Server included, and integral to, DRRS. The server will exchange and maintain data from the GFM Organization Servers (Service, Joint, and DoD-level) as required to support DRRS functionality.
Doctrinal Organization	GFM DI	The arrangement or hierarchical grouping of organizations that support a mission. Organizations needed for mission areas, functions, doctrine, tactics, techniques, and procedures are routinely used for mission accomplishment and must be documented in the OFSC.
DoD Component	CJCSI 3170.01	The DoD components consist of the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the DoD, the Defense agencies, DoD field activities and all other organizational entities within the DoD.
Enterprise	GFM DI	The Department of Defense, its organizations, and related Agencies. Also, a defined functional and administrative entity that exists to perform a specific, integrated set of missions and achieve associated goals and objectives, encompassing all of the primary functions necessary to perform these missions. Note – an enterprise may also be defined by use of identifiers (i.e., the Enterprise that consists of systems that utilize EwIDs for data exchange is defined by use of the EwIDs).
Equipment	DoD	A specific piece of materiel.
Extensible Markup Language (XML)	DoD CIO Net-Centric Data Strategy	A tagging language used to describe and annotate data so it can be consumed by human and system interactions. XML is typically arranged hierarchically using XML elements and attributes. It also uses semantically rich labels to describe elements and attributes to enable meaningful comprehension. An example of XML data describing an element named “Person” appears as follows: <pre data-bbox="540 1444 984 1619"><Person> <FirstName>John</FirstName> <MiddleInitial>H</MiddleInitial> <LastName>Doe</LastName> </Person></pre>
FMIDS Seeds Server	OFSC FMIDS Management Plan	The FMIDS Seed Server will be the single source for managing and issuing the seed prefixes required for the generation of FMIDS within the GFM Domain. This will be the same FMIDS Seed Server that issues the seeds used to generate FMIDSs outside the GFM network. Some features of the FMIDS Seed Server are: - Provide Seed Allocation Service (SAS) via a web application interface which manages the requests for and allocation of FMIDS Seeds

Term	Definition Source	Definition
		- A seed allocation Tracking Service (TS) via web services interface which FMIDS Servers (FS) to programmatically identify the POC for a particular seed.
FMIDS Servers (FS)	GFM DI	Any computer program that provides FMIDS to requestors. Creates an FMIDS by obtaining EwID seed and appending a locally generated suffix to the EwID seed (prefix).
Force Management	FM FCB	An organizing construct of processes, policies, organizational information, and tools that informs senior leader decision making on the global joint sourcing of the Defense Strategy.
Force Management Identifier (FMIDS)	GFM DI	A member of a set of attributes in the GFMIEDM that serve as EwIDS for its components (i.e., entities or tables) or the set of attributes that are EwIDS for GFMIEDM components (i.e., entities or tables).
Force Structure	GFM DI, DoDI 1120.11	The organizations, units, personnel and equipment that comprise the Department of Defense. A unit is defined as a military element with a structure prescribed by competent authority, such as a table of organization and equipment or a manning document. Includes unit requirements for both manpower and equipment resources. The totality of units in a DoD Component.
Global Force Management (GFM)	GFM GUIDANCE (4 May 2005)	<p>GFM aligns force apportionment, assignment, and allocation methodologies in support of the National Defense Strategy and joint force availability requirements. It provides comprehensive insights into the global availability of U.S. military forces and provides senior decision makers a process to assess quickly and accurately the impact and risk of proposed changes in forces / capability assignment, apportionment, and allocation. GFM goals are to:</p> <ul style="list-style-type: none"> · Account for forces and capabilities committed to ongoing operations and constantly changing unit availability. · Identify the most appropriate and responsive force or capability that best meets the combatant command requirement. · Identify risk associated with sourcing recommendations. · Improve ability to win multiple overlapping conflicts. · Improve responsiveness to unforeseen contingencies. · Provide predictability for rotational force requirements.
Global Force Management Information Exchange Data Model	DoDI 8260.03 (August 23, 2006)	An augmented subset of the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM), formally known as the “Command and Control Information Exchange Data Model (C2IEDM)”. JC3IEDM is part of Standardization Agreement (STANAG) 5525 which currently under ratification by NATO. It is a set of information elements, entities, and relations that describe the information exchange requirements within military operations. The GFMIEDM is a reference model used to exchange information between two systems to reach a common understanding of the data.
Global	DoDD	The globally interconnected, end-to-end set of information capabilities,

Term	Definition Source	Definition
Information Grid (GIG)	8100.1, Sep. 19, 2002	associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid (GIG) includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense (DOD), National Security, and related intelligence community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.
Interoperability	DoDD 4630.5	The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle and must be balanced with information assurance.
Metadata	DoD CIO Net-Centric Data Strategy	Descriptive information about the meaning of other data. Metadata can be provided in many forms, including XML.
Metadata Registry	DoD CIO Net-Centric Data Strategy	A system that contains information that describes the structure, format, and definitions of data. Typically, a registry is a software application that uses a database to store and search data, document formats, definitions of data, and relationships among data. System developers and applications are the predominant users of a metadata registry.
Materiel	DoD	All items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. Class-2 Materiel = "Equipment". See also Equipment.

Term	Definition Source	Definition
Net-Centric Enterprise Services (NCES)	GFM DI	NCES will provide Department of Defense (DoD) organizations ubiquitous access to reliable, decision-quality information through a net-based services infrastructure and applications to bridge real-time and near-real-time communities of interest (COI). NCES will empower the edge user to pull information from any available source, with minimal latency, to support the mission. Its capabilities will allow GIG users to task, post, process, use, store, manage, and protect information resources on demand for warriors, policy makers, and support personnel.
Organization	EDI	An organized entity within the military. The entity can be defined as any doctrinal organization and all its subordinate organizations. For example, an Army Unit of Action is an organization. A UA is composed of several battalions, each of which is an organization, as well. The last nodes in an organization are always billets.
Organizational and Force Structure Construct (OFSC)	DoDI 8260.3	A hierarchical framework used to organize (document) force structure data for joint integration within, and across, organizational boundaries. Includes the concept and tenets that provide common semantics and rules for documentation, displayed in a “top-to-bottom” hierarchical structure, together with the operational aspects (Tactics, Techniques, and Procedures), and is available from a single authoritative data source (called an “Organizational Server”) for use by multiple enterprise programs (readiness, personnel, manpower, command and control, etc.). Originally called the Force Structure Construct (FSC) .
Organizational and Force Structure Construct (OFSC)	GFM DI Draft DoDD 8260.03 (August 23, 2006)	A joint hierarchical way to organize (document) force structure data for integration within and across organizational lines. Includes the concepts and tenets that provide common semantics and rules for documentation, displayed in a “top-to-bottom” hierarchical structure, including the operational organizational aspects (Tactics, Techniques, and Procedures), and is available in an organizational server for use by multiple enterprise programs (DRRS, DIMHRS, C2, etc.). Originally called the Force Structure Construct (FSC) .
Organizational Structure		The alignment and design of military units in order to best use available resources and to provide for a seamless transition from peace to war. This concept provides for a clear chain of command running from the President to the most junior soldier, sailor, airman, and marine.
OSD Organizational Server	GFM DI	The authoritative repository for organization information for those organizations not included in the Service Organizational Server (SOS) or Joint Organizational Server. The components of the DoD-level Organizational Server include: the Office of the Secretary of Defense, the Office of the Inspector General of the DoD, the Defense agencies, DoD field activities and all other organizational entities within the DoD and outside of DoD required to support DoD missions
Schema	DoD CIO Net-Centric	Schema is a diagrammatic representation, an outline, or a model. In relation to data management, a schema can represent any generic model or structure that

Term	Definition Source	Definition
	Data Strategy	deals with the organization, format, structure, or relationship of data. Some examples of schemas are (1) a database table and relationship structure, (2) a document type definition (DTD), (3) a data structure used to pass information between systems, and (4) an XML schema document (XSD) that represents a data structure and related information encoded as XML. Schemas typically do not contain information specific to a particular instance of data.
Unclassified Environment	OFSC FMIDS Management Plan	Computer and networking systems (collectively referred to as Automated Information Systems (AIS)) used to capture, create, store, process or distribute information that does not meet requirements to be designated as classified, but must be operated so that the information is protected against unauthorized disclosure or modification.
Unique Identification	GFM DI	A system of establishing globally ubiquitous unique identifiers within the Department of Defense, which serves to distinguish a discrete entity or relationship from other like and unlike entities and relationships.
Unique Identifier (UID)	GFM DI	A character string, number or sequence of bits assigned to a discrete entity or its associated attribute which serves to uniquely distinguish it from other like and unlike entities. Each unique identifier has only one occurrence within its defined scope of use.
Web Service	DoD CIO Net-Centric Data Strategy	Web services are self-describing, self-contained, modular units of software application logic that provide defined business functionality. Web services are consumable software services that typically include some combination of business logic and data. Web services can be aggregated to establish a larger workflow or business transaction. Inherently, the architectural components of web services support messaging, service descriptions, registries, and loosely coupled interoperability.

Appendix G – References

CJCSI 3170.01 – Joint Capabilities Integration and Development System, May 2005

Concept of Operation for an Enterprise-wide Identifier Seed Server (ESS), June 2005

DIMHRS (Manpower) – Way Ahead Document, Mar 2005

DoDD 5124.2 – Under Secretary of Defense for Personnel and Readiness, Oct 1994

DoDD 8320.2, Data Sharing in a Net-Centric Department of Defense, December 2, 2004

DoDD 8320.03 – Unique Identification for a Net-Centric Department of Defense, March 2007

DoDI 7730.64 – Automated Extracts of Manpower and Unit Organizational Element Files, Dec 2004

DoDI 8260.03 – Organizational Force Structure Construct (OFSC) for Global Force Management (GFM), August 2006

Draft Global Force Management Data Initiative (GFM DI) Concept of Operations, July 2006

Global Force Management (GFM) Force Management Identifiers (FMIDS) Management Plan, March 2007 (draft)