DoD Manual 8260.03, Volume 1

Global Force Management Data Initiative Implementation: Unique Identification for Enterprise Force Structure Data

Originating Component:	Office of the Under Secretary of Defense for Personnel and Readiness
Effective:	July 1, 2022
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Manual 8260.03, Volume 1, "Global Force Management Data Initiative (GFM DI) Implementation: Unique Identification (UID) for GFM," November 20, 2009
Approved by:	Thomas A. Constable, Performing the Duties of the Assistant Secretary of Defense for Manpower and Reserve Affairs

Purpose: This manual is composed of two volumes, each containing its own purpose. In accordance with the authority in DoD Directive 5124.10 and the guidance in DoD Instruction (DoDI) 8260.03:

- This manual implements policy, assigns responsibilities, and provides procedures for the generation of enterprise force structure (EFS) data across the DoD.
- This volume assigns responsibilities and prescribes procedures for the unique identification (UID) of EFS data, including:
  - Use of the enterprise-wide identifier (EwID) technical schema for global force management identifier (GFMID) generation
  - Acquisition of seed values (EwID prefixes) from the centrally managed enterprise seed server (ESS).
  - Configuration and tracking requirements of GFMIDs.
  - Use of GFMIDs to fulfill the organization unique identifier (OUID) mandate of DoDI 8320.03.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This volume applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

In accordance with DoDI 8260.03, it is DoD policy that the Global Force Management Data Initiative (GFM DI) must provide a digitized, hierarchical baseline of EFS data for end-to-end integration across DoD functional areas. Enterprise-wide integration of discrete EFS data is enabled by use of unique identifiers called GFMIDs. All DoD GFM DI EFS data elements are associated with a unique GFMID. Those GFMIDs used to uniquely identify specific DoD organizations at any level also implement the OUID mandate of DoDI 8260.03.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)).

The USD(P&R):

a. Assists the Director for Force Structure, Resources, and Assessment, Joint Staff J-8, in policy development and implementation oversight of this issuance, in coordination with other OSD Component heads, and DoD Component heads, and in accordance with DoDI 8260.03 and this volume.

b. Coordinates the linkage of GFMIDs with other unique identifiers explicit throughout the DoD enterprise to enable data discovery, correlation, and sharing of information in accordance with DoDIs 4165.14, 8320.02, 8320.03, and 8320.04.

c. Generates and manages all EFS data under OSD control, with the exception of EFS data under the purview of the Under Secretary of Defense for Intelligence and Security (USD(I&S)).

2.2. USD(I&S).

The USD(I&S) generates and manages all EFS data under USD(I&S) control.

2.3. SECRETARIES OF THE MILITARY DEPARTMENTS AND THE COMMANDANT OF THE U.S. COAST GUARD.

The Secretaries of the Military Departments and the Commandant of the U.S. Coast Guard:

a. Develop and distribute guidance to implement this issuance in their Components.

b. Generate and manage all EFS data under that Military Department's control. For the U.S. Coast Guard, the provisions of this issuance only apply to those elements of force structure relevant to global force management (GFM) processes for performing DoD missions under Title 10, United States Code.

2.4. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

The Chairman of the Joint Chiefs of Staff:

a. Centrally manages and oversees the GFM DI.

b. Develops and distributes policy and guidance to implement this issuance, in coordination with the USD(P&R).

c. Coordinates with OSD and DoD Component heads in the decentralized execution of GFM DI objectives.

SECTION 3: UID REQUIREMENTS FOR EFS DATA

3.1. OVERVIEW.

a. General Context.

(1) GFM DI is centrally managed by the Joint Staff Directorate for Force Structure, Resources, and Assessment (J-8), and decentrally executed by a collaborative community of interest that includes partners from the Military Services, the OSD, the joint community, and DoD elements of the Intelligence Community.

(2) GFM DI technical products are cited in the DoD Information Technology (IT) Standards Registry pursuant to DoDI 8320.02. The EFS baseline authoritative data sources (ADSs) are organization (org) servers populated and maintained by the DoD Components in accordance with GFM DI technical guidance and DoDI 8260.03.

(3) In accordance with DoD Directive 8000.01 and DoDI 5015.02, information is a strategic asset. It must be appropriately secured, shared, and made available throughout the information life cycle to any DoD user or mission partner to the maximum extent allowed by law. Any system reliant on multiple information sources must be able to link together disparate data and information via relationships. Pursuant to DoDI 8320.03, UID of discrete data is directed throughout the DoD enterprise to modernize the IT systems of DoD Components and their mission partners. Assigning unique identifiers to data enables the referencing of otherwise arbitrary pieces of information across disparate information systems with minimal prior coordination.

b. General Properties of Unique Identifiers.

There are four preferred properties associated with unique identifiers in general:

(1) Unintelligent.

The primary identifier is unsusceptible to change. Nothing in the construct of the identifier is dependent on characteristics of the data it tags, therefore future changes in the data itself have no impact on the identifier. The same piece of data should never change its primary identifier.

(2) Exchanged as a Single Attribute.

The identifier is not composed of parts imported from other tables. It is a fixed singular construct that is unsusceptible to change once instantiated by an authoritative source of record.

(3) A Fixed Size.

To facilitate ease of implementation for software developers, the identifier should be a fixed size common to computing hardware, such as a number of bytes aligned to an 8-bit frame.

The size of the address space dictates the amount of bandwidth required for efficient sharing as well as an upper limit on the quantity of available identifiers.

(4) A Consistent Distribution Scheme.

Generating unique identifiers may occur via strategies that are centralized, decentralized, or a combination of both.

(a) In a centralized scheme, every unique identifier is controlled by a dominant authority. This requires a user to contact an external source as a routine part of the generation process. The central authority ensures non-duplication in that portion of the identifier it provides to ensure uniqueness across the enterprise.

(b) In a decentralized scheme, the unique identifier is created completely locally. This allows the possibility of independent users generating duplicate values. The probability of duplication decreases as the identifier size increases. A decentralized approach has the advantage of user independence from the possible delays of a centralized service. The cost is a lengthier identifier and the challenge of determining where any out-of-context identifier originated.

(c) A combination of both schemes joins a centrally managed prefix, called a seed, with many locally managed suffixes. GFM DI implements this approach.

3.2. GFM DI REQUIREMENTS.

The UID schema for GFM DI must fulfill the requirements in Paragraphs 3.2.a.– e.:

a. Optimize the construct of the identifiers so that they are purely for data identification and not used to encode information from a reference table in a hardcopy publication. This liberates the data from category restrictions imposed by 26 letters or the digits 0 through 9.

b. Ensure viable implementation to support integration of EFS data by a wide variety of older, legacy applications in any operating system, regardless of database format.

c. Enable usability over narrow bandwidth systems and limited wireless environments. To reach the full potential of data exchange described in DoDI 8260.03, the identifier length is restricted to 64 bits (8 bytes). At this size, a degree of centrally managed oversight is required for uniqueness.

d. Promote policy and technical modifications that permit the new UID schema to become at least an alternative, and ultimately the primary reference, for extant data in local data stores.

e. Use an automated tracking ability to facilitate queries and establish the identifier's system of origination.

SECTION 4: THE EWID

4.1. DESCRIPTION.

The EwID is the chosen UID standard used to generate GFMIDs for EFS data.

a. EwID Properties.

The EwID schema satisfies GFM DI unique identifier requirements for interoperability and ease of software development. The EwID is:

(1) Unintelligent, as described in Paragraph 3.1.b.(1) of this volume.

(2) Exchanged as a single attribute completely independent of any operating system interactions, as described in Paragraph 3.1.b.(2) of this volume.

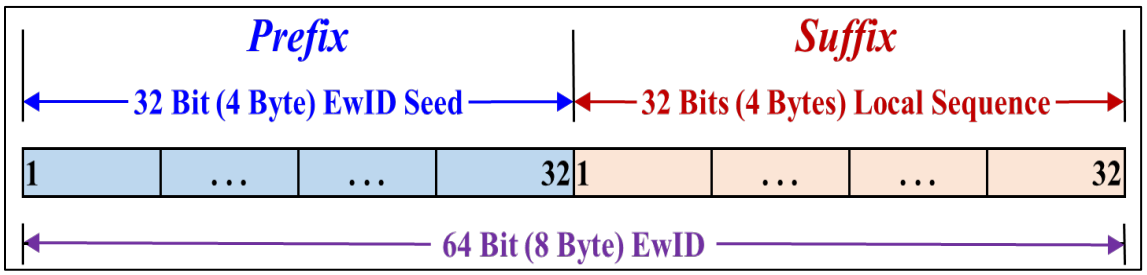
(3) A fixed size (64 bits) suitable for low bandwidth environments in accordance with Paragraph 3.1.b.(3) of this volume.

(4) Implemented by a combined distribution scheme, as described in Paragraph 3.1.b.(4) of this volume.

b. Technical Implementation.

(1) A common method for producing globally unique values is by concatenating two smaller values. In the EwID schema, one of those values is a 32-bit prefix (a "seed") provided from the ESS. An assigned seed is always unique. The receiving office of primary responsibility (OPR) manages the generation of full 64-bit EwIDs by concatenating locally produced suffixes to its assigned 32-bit seed(s) (see Figure 1) using a "concatenator."

Figure 1. Concatenation of a 64-bit EwID



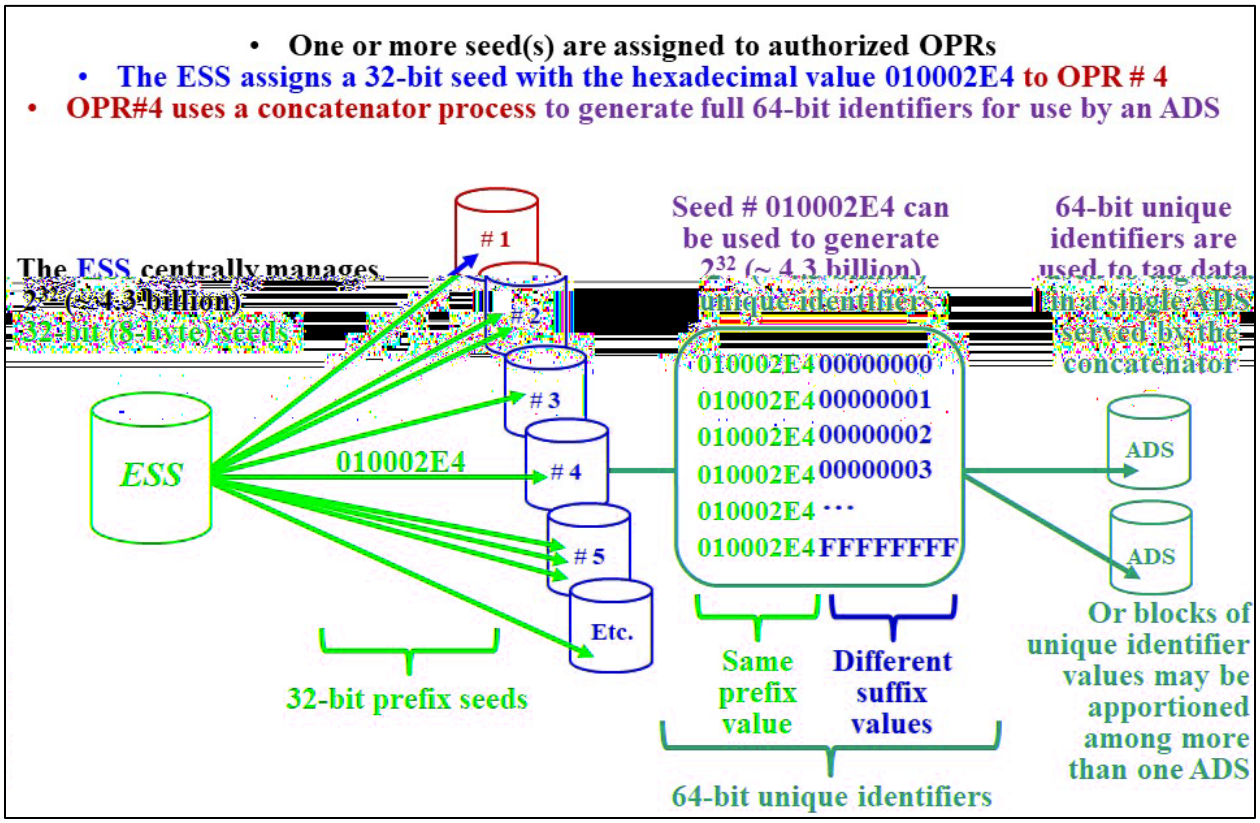
(2) The seed value allows an OPR for any 64-bit value to be determined, while allowing an OPR independence in generating full 64-bit identifiers based on the seed(s) assigned to them.

(3) As an OPR creates new data, a newly generated EwID tags it. A given EwID is a perpetual label that is never recycled to tag some other data. To avoid duplication, any EwID

OPR must ensure its concatenator mechanism abides by the EwID generation rules described in this volume.

(4) Figure 2 illustrates the EwID distribution architecture and distinguishes the roles of an ESS, a 32-bit seed, a concatenator, and a fully formed 64-bit identifier. The EwID distribution has three levels of operation. On the left of Figure 2 is the ESS, in the middle are local concatenators, and on the right are EwID users assigning identifiers to data within one or more ADSs. End users generating new data, often in a database, obtain new EwIDs from their local concatenator and not directly from the ESS.

Figure 2. EwID Distribution Architecture



(5) An address space of 32 bits means that the ESS can parcel out 2^{32} seeds (i.e., 4.3 billion rounded off), which is the total possible combinations in a fixed-length sequence of 32 ones and zeroes. Each seed is capable of supporting approximately 4.3 billion suffixes, for a total range of 2^{64} EwIDs. The upper mathematical limit in binary notation is 64 ones. This equates to 16 "F"s in hexadecimal notation, or a 20-digit integer in decimal notation: 18,446,744,073,709,551,616 (rounded off as 18.4 quintillion, or 18.4 billion billions if using the long scale).

4.2. OBTAINING EWID SEEDS.

a. Procedures.

(1) An ESS user account is required for an authorized OPR to obtain EwID seeds. The GFM DI ESS Intellipedia Website provides instructions for contacting the ESS administrator for this purpose. An OPR must, as prerequisites for account approval:

(a) Provide and maintain information for a point of contact (POC).

(b) Guarantee that its concatenator process generates 64-bit EwIDs using only authentic seed values assigned from the ESS.

(c) Use a mechanism to prevent duplicate EwIDs, to include a backup scheme to prevent reuse of EwIDs in the event of a power loss or major malfunction.

(2) The ESS administrator evaluates the request. Once approved, the ESS administrator provides the seed account, seed(s), or both, as applicable, via e-mail to the OPR POC.

(3) Management of repeat requests for additional seed values follow the same procedures as the initial request. An OPR may request more than one user account to support management of multiple end users or security considerations.

b. Users.

The enterprise of ESS account holders is not restricted to the org servers nor is it constrained by Military Service, governmental, or national boundaries. The Joint Staff encourages the widespread use of EwIDs to enhance DoD data exchange and interoperability.

c. Usage Levels.

(1) An OPR should receive as many seeds as required, but no more. Users are encouraged to be efficient and may increase their usage level as necessary without creating a new account.

(2) Possible reasons for requiring more than one EwID seed are database performance and the management of multiple systems, each with its own dedicated concatenator. The data source dispersion problem can be solved in different ways depending upon estimated requirements and leveraging of surrogate key flexibility.

(3) Data sources tightly coupled over a high bandwidth communications environment may use a single concatenator with a single seed to serve many systems without degradation. In this case, a concatenator partitions the locally controlled EwID suffix into blocks. For example, the approximately 4.3 billion EwID suffixes could be broken into 100 EwID blocks of 43 million each and dispersed into 100 distributed systems. As a system nears the end of its block of EwID, the manager must obtain a new EwID seed and create another set of blocks to be distributed.

d. EwID Tracking.

The ESS process of sequential assignment of EwID seeds prevents duplication. Furthermore, maintaining current contact information for EwID seed assignment supports user discovery of additional information from any EwID.

SECTION 5: THE GFMID

5.1. DESCRIPTION.

The term "GFMID" is applicable for all EwIDs that tag EFS data. This includes both the baseline EFS data generated by org servers as well as in consumer systems of org server data that generate temporary links or nodes (data aggregation points) for documenting dynamic, task-organized forces.

a. Technical Implementation.

GFMIDs uniquely tag data generated using the GFM extensible markup language schema definition (XSD).

(1) Every record requires a GFMID as a primary key.

(2) The GFM XSD and related technical products and guidance may be accessed from the Intellipedia site of the GFM DI configuration control board. The GFM XSD provides the information exchange specification for EFS data deemed to be minimally essential by the GFM community of interest and made accessible to authorized users and applications via the suite of org servers.

b. GFMID Generation.

GFMID generation requires an OPR to acquire at least one 32-bit EwID seed from the ESS. The OPR creates GFMIDs only from ESS assigned seeds and must prevent duplicated GFMIDs.

(1) The OPR for that seed establishes a concatenator to produce full 64-bit identifiers.

(2) The OPR has ownership of the GFMID under the rules described in this volume (e.g., all suffixes are unique per seed).

5.2. GFMID TRACKING CONCEPT OF OPERATIONS.

It is possible that a data payload may provide GFMIDs without including the data they reference. For this reason, a GFMID tracking service allows discovery of a given GFMID's OPR, based on the seed value, for further investigation and potential querying. A uniform resource identifier (URI) may accomplish this end. A URI can be a uniform resource locator (URL), a uniform resource name (URN), or both. If the network employs universal description, discovery, and integration (UDDI) services, then every URI must use a URN. A URN can span many networks by mapping to different URLs via the UDDI registry in each network.

a. Tracking High-Level Design.

The ESS enables the ability to track down a GFMID OPR by determining its seed assignment. Automation of the tracking process requires viable URIs that forward queries to an

OPR. There are no stipulations as to how a "tracker" is coupled with an ADS or the extent of the information provided. However, a tracker service must exist that follows the defined protocols of this volume. An OPR has maximum flexibility in configuring and controlling its tracking service within the context of the high-level guidance in Paragraphs 5.2.a.(1)-(7) of this volume.

(1) GFMID seed tracking is a mandatory subset of GFMID tracking. The OPR of a given GFMID must be discoverable from its seed value even without further information of what the GFMID references.

(2) A tracker returns information about a GFMID in response to a user query. The information may be:

(a) About the owner of the data;

(b) The data itself;

(c) Further guidance as to how to locate the ADS (via a URL or URN); or

(d) How to acquire access to the ADS, if applicable.

(3) The information provided may be resident within the source whose tracker has been interrogated, or it may reside in another source for which one or more tracker redirection(s) has occurred. This redirection may be hidden from the user. Tracker design and placement is flexible and determined by the seed OPR.

(4) GFMID tracking can be initiated on any tracker. External customers may contact the ESS or ESS administrator to identify the seed OPR and the URI for the next tracker in the sequence, as applicable. This process may or may not be automated.

(a) If no URI exists, only the POC information submitted by the account holder is provided, hence the necessity of OPRs maintaining current POC information.

(b) In the event that the GFMID queried is based upon a seed never assigned to a seed account, this information is also provided to the requestor.

(5) In a sequence of cooperative trackers, an automated process may continue to forward a GFMID tracking request as long as valid URIs are provided. Eventually, the request arrives at the ADS where the GFMID was generated to tag data. At this point, at the discretion of the ADS owner, the GFMID is identified in one of several ways:

(a) The GFMID itself is identified as "Not Valid."

(b) The information identified by the GFMID is returned to the requestor.

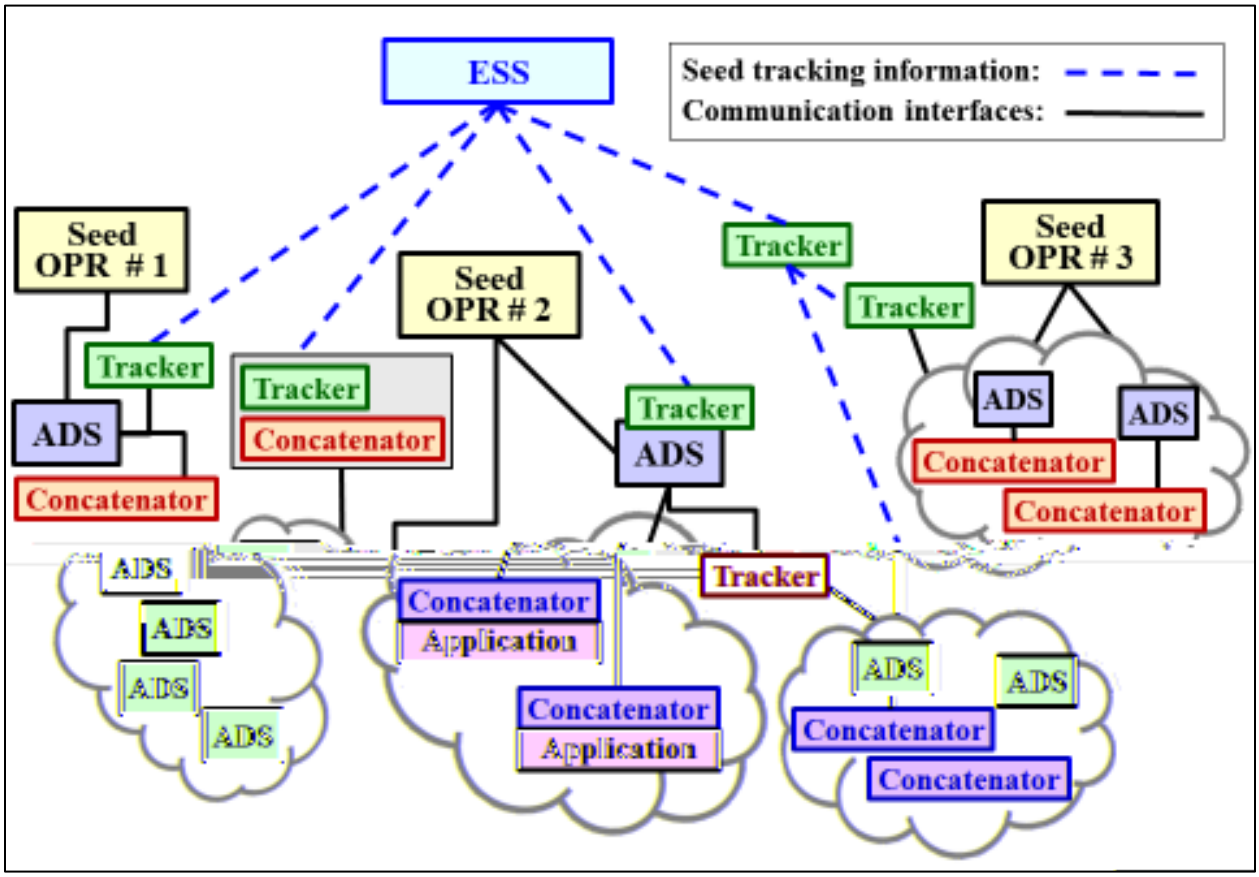
(c) A refusal message is sent.

(6) The interconnectivity of any sequence of cooperative tracker applications should be transparent to the user performing a query. The user should receive an answer from the

authoritative source at the end of any sequence of trackers as if the answer came immediately from the system used to initiate the query.

(7) Figure 3 illustrates examples of alternative configurations for placement of trackers and concatenators for seed distribution. These examples are not comprehensive. For any chosen arrangement, every node in the prefix redirection hierarchy must have its own concatenator and tracker for its data source. This is regardless of whether the node is an org server or any other application generating GFMIDs for EFS data purposes.

Figure 3. Examples of Possible GFMID Distribution and Tracking



b. GFMID Statuses.

For OPRs not producing EFS data, participation in the GFMID tracking service is optional. To manage GFMIDs for GFM DI, participation is required. Paragraphs 5.2.b.(1)-(3) of this volume describe seed statuses throughout the tracking process.

(1) Assigned and Redirected.

A seed is assigned to an OPR, which must generate complete 64-bit GFMIDs locally. An OPR may elect to use more than one concatenator for this purpose, such as a master service with one or more cooperative concatenators. In this case, the term "redirection" refers to when a seed passes through multiple concatenators prior to full GFMID generation. There is no limit to the

number of times that a seed or GFMID may be redirected to a cooperative concatenator. A given seed may have its possible suffixes partitioned into blocks of values for redirection to multiple other concatenators. Every OPR that redirects a seed or a GFMID block must implement an accompanying tracker that ultimately locates the data source that first used the applicable GFMID.

(2) Active and Inactive.

Within a given concatenator, seeds are "inactive" by default until actually used to generate a GFMID.

(a) A concatenator from which a seed has been redirected labels that seed as active. This ensures that a GFMID search continues regardless of how many times its seed has been redirected. Each subsequent server that redirects the seed also marks it as active until reaching the final end user in the redirection chain.

(b) Only at the last tracker, where a concatenator is often collocated, would an unused seed be marked as inactive pending further action.

(c) A seed becomes "active" once it generates a single GFMID.

(d) The purpose of the designation "active" is twofold. It may indicate that there are no further links in a redirection sequence and that the seed has generated GFMIDs. Alternatively, it may indicate that the current concatenator is not the last link of a sequence and a query needs forwarding to the next level.

(e) All GFMID owners at every link in the seed redirection chain are responsible for tracker responsiveness to enquiries from authorized requestors. They are also responsible for ensuring the traceability of the seed(s) they manage, to resolve queries regarding GFMIDs they generated.

(3) Seed Revocation.

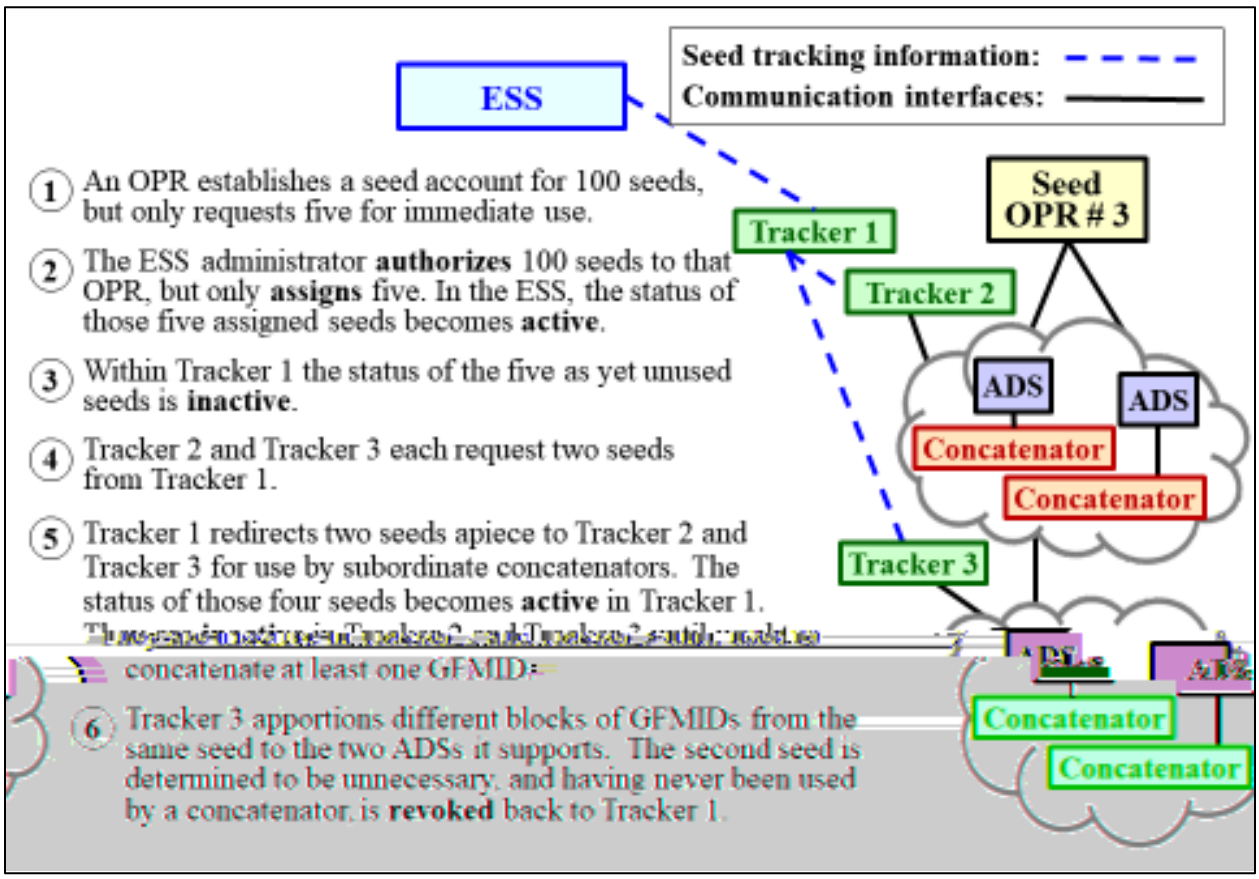
In the case that an end user obtains more seeds than ultimately needed, any seed never used may be "revoked" to an alternative source. This source might be an alternative end user or a regression to a more senior tracker, including back to the ESS.

(a) Within a sequence of cooperative trackers, each new user level to which an unused seed is revoked changes its status from active to inactive.

(b) A seed once used to generate GFMIDs must never return to inactive status at any user level. Consequently, a seed once activated through GFMID generation may never be revoked. Only an unused seed may revert from active to inactive status via the revocation process.

(c) Figure 4 illustrates the use of GFMID distribution terminology.

Figure 4. Definitions for GFMID Seed Distribution



5.3. GFMID PERSISTENCE.

A GFMID generated to tag an EFS record in accordance with GFM DI technical artifacts remains with that record permanently. As records become obsolete, their retained GFMIDs enable the work of discovery services inside of historical archives.

5.4. OPR RESPONSIBILITIES FOR GFMID GENERATION.

Any organization serving as an OPR for GFMID generation has three sets of responsibilities: to the ESS administrator, to the data sources requiring the generation of GFMIDs, and to external consumers of the EFS data under the support of that OPR.

a. GFMID generating OPRs must:

(1) Maintain accurate POC and URI information in the ESS. The ESS administrator uses the URI to provide the initial location to begin the search for the source of the GFMID.

(2) Use only the seeds assigned from the ESS to produce concatenated 64-bit GFMIDs.

(3) Assign the status of "active" to any seed used to generate at least one GFMID.

(4) Maintain a mechanism to prohibit duplication of GFMIDs by any concatenator under its control. This includes an emergency backup scheme in case of interruption of GFMID generation and tracking services.

(5) Maintain an internal tracking service that:

(a) Ensures intercommunication with any cooperative concatenator.

(b) Ensures the uniqueness of each GFMID.

(c) Provides POC information about all trackers and concatenators.

(d) Provides a lookup service to return data associated with the GFMID, when queried from any authorized system.

(6) Ensure that all data provided to consumers retains its originally assigned GFMID.

b. No GFMID may be changed by an EFS data consumer.

5.5. GFMIDS ACROSS SECURITY DOMAINS.

As an unintelligent identifier, a GFMID provides no information regarding the security classification of the record that it identifies. Information security marking metadata associated with every record serves this purpose. A GFMID is but one attribute of a record with multiple other attributes, and shares the classification of the overall record in accordance with DoD policy on data compilation.

a. In accordance with DoDI 8260.03, data should be originally created in the domain equivalent to its classification. Therefore, unclassified data should always be created in an unclassified domain for replication to higher security domain, where the original GFMID is retained. Unclassified data elements may retain their unclassified marking after replication to a higher domain and augmentation with classified data, as applicable in accordance with DoD classification standards.

b. Although the ESS is unclassified, seeds may be designated for use solely at higher security domains. The ESS documents seeds that are assigned in any higher security domain but does not record any further information. A concatenator in a higher security domain operates in the identical manner as one in an unclassified domain.

c. The same seed must not be used for generating GFMIDs in different security domains. However, legacy practices and operational demands result in the generation of unclassified data in classified domains (or of secret data in a top-secret domain). In these circumstances, records generated in a higher security domain are never passed to a lower domain without confirmation that their classification metadata is commensurate to that of the destination. The only full 64-bit GFMIDs ever encountered in an unclassified domain that were concatenated from a seed assigned to a classified domain concatenator must be for unclassified data cleared for transfer into that lower domain.

d. UDDI services are particularly valuable when the networks span security domains. In this situation, a URN can span many networks and map to different URLs in each network UDDI registry.

SECTION 6: THE OUID

6.1. DESCRIPTION.

GFM DI maps the hierarchy of military organization to the tree graph terminology of nodes and links. Nodes are aggregation points for additional data. They may represent the doctrinal size or echelon of a unit (e.g., a battalion or squadron), a crewed platform authorization (e.g., the crew of a plane, tank, or ship), or a single billet. Generically, GFM DI calls such nodes "organizational elements" (OEs). To avoid duplicative efforts, GFMIDs that uniquely identify OEs fulfill the OUID mandate of DoDI 8320.03.

a. Distinctions between an EwID, a GFMID, and an OUID.

(1) An EwID is:

(a) A method of UID.

(b) A 64-bit UID composed of:

1. A 32-bit prefix called a seed, generated by the centrally managed ESS.

2. A 32-bit suffix locally generated by the OPR assigned a unique seed by the ESS.

(2) A GFMID is an EwID that is used exclusively for EFS data.

(3) An OUID is a GFMID used exclusively for OE records (i.e., organizations, units, platforms, or billets).

(4) GFMIDs used for identifying non-OE records (e.g., links between nodes, type characteristic details, or instances of objects other than OEs) are not OUIDs.

b. Scope.

The EFS baseline data (i.e., DoD force structure at rest) is published from the org servers for consumption and augmentation in external consumer systems. Such systems include those that require additional force structure elements to document dynamic task organizations or aspects of the DoD total force beyond the baseline authorizations. Such data should also eventually conform to EFS data standards, to include the generation and use of GFMIDs and OUIDs.

6.2. OUID CONCEPT OF OPERATIONS.

a. OUID Generation.

The GFM DI org servers are the ADSs for all OUIDs that originate in the EFS baseline.

(1) OUID generated for force management of dynamic, task-organized units may be generated in applicable Military Service or joint IT systems that support the GFM allocation process (e.g., the Global Laydown Server).

(2) All new systems that share organizational data must integrate the OUID.

(3) The OUID does not supersede existing interoperable data exchange standards listed in the DoD IT Standards Registry, but compliments them to facilitate their use across the DoD. The OUID does not replace identifiers used to support existing policies, agreements, and practices internal to the DoD (e.g., unit identification code (UIC), personnel accounting symbol (PAS), or reporting unit code (RUC)) or external to the DoD (e.g., U.S. Treasury Account Number or the Data Universal Numbering System).

b. OUID Properties and Rules.

(1) Non-Duplication Properties.

Components must conduct checks to ensure that:

(a) An OUID is assigned to only one OE.

(b) An organization is not assigned more than one OUID at any one time.

(c) An OUID, once used, is never reused.

(2) Retention Rules.

An EFS data consumer system's ability to associate its own data with an OUID is the driving factor behind the necessity of OUID retention. To this end, the GFM XSD permits changes to many OE characteristics to occur elsewhere than the OE record itself (e.g., an alias).

(a) Any change in a superior OE does not necessitate changing the OUIDs of its subordinate OEs if their inherent attributes are unchanged. This is due to GFM DI treating a unit as an aggregation of separately identified parts, and not as a unified entity such as occurs with a UIC.

(b) An OE has start and termination date-time attributes that define when the OE is active. The move from one fiscal year to the next does not necessitate a change in OUID, since an OE's timespan may be of long and unknown duration. GFM DI defines a default termination date in the far future for this reason. Changing an existing termination date value for an OE does not necessitate a new OUID. For example, an OE expected to expire at the end of the current fiscal year but then extended may update its termination date without requiring a new OUID.

(c) After an OE's termination date has passed, the OUID and associated data must not be deleted. They must be retained for historical purposes in accordance with DoDI 8260.03.

(d) The GFMID OPR determines when changes to an OE warrant retiring the current OUID (and archiving the associated obsolete data) and generating a new OUID with new attributes for publication to consumers.

(3) External Billet OUID Management.

(a) An external billet is a billet authorized to one organization that, via workforce agreements, fulfills its routine duties within the hierarchy of a completely different organization. The billet is under the direction and control of the gaining organization, but remains owned by the providing organization for administrative purposes. Examples include:

1. Service billets embedded within units of a different Military Service (e.g., Navy Corpsmen in Marine Corps units).

2. Service billets within OSD defense agencies or DoD field activities.

3. Service billets within inherently joint organizations.

(b) The GFM DI configuration control board Intellipedia site hosts detailed business rules for external billet management.

c. OUID Implementation Policy.

In accordance with DoDIs 8320.03 and 8260.03, the OUID provides the means for the DoD to migrate to a single organization identifier scheme across the DoD enterprise for information discovery and sharing. The OUID will not supersede, but rather complement, existing accepted international interoperable data exchange standards for globally UID of organizations.

(1) New System Implementation.

All new systems will be developed with the capability to use OUIDs within that system and to use it when interfacing organizational information.

(a) Implementation of OUIDs across the DoD enterprise must be in accordance with the system processes as outlined in applicable DoD issuances, Component directives, and system technical direction (e.g., DoDIs 8320.06 and 8320.03).

(b) Strict adherence to the rules for generating and maintaining an OUID is required to ensure that it uniquely identifies only one organization across the DoD enterprise. This enables access to organizational-based data in diverse sources without maintaining lookup, crosswalk, or conversion tables.

(c) Current policies, practices, and agreements with organizations outside of the DoD will still require the use of other organization identifiers (e.g., UIC, PAS, or RUC) in addition to the OUID.

(2) Legacy System Implementation.

(a) An OPR may choose to implement the OUID as the single organization identifier within their legacy system.

(b) Legacy systems may also look up the OUID based on organization aliases and use the OUID when interfacing organizational information. The objective is to minimize the impact on legacy systems by providing the most efficient means of incorporating the use of OUID into these systems.

(c) If a system must link existing organization identifiers (e.g., UIC, PAS, or RUC) to an applicable OUID, then a lookup process must support it.

(d) For an organization identifier used by multiple systems, the authoritative source of the identifier should also be the authoritative source for mapping it to the OUID. If only a single system uses a specific organization identifier internally, then such mapping must also occur internally.

(3) OUID Tracking.

Since the OUID is a subset of GFMIDs, the prefix of an OUID may be used to identify the source of the data via the tracking process described in Paragraph 5.2. of this volume.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
ADS	authoritative data source
DoDI	DoD instruction
EFS	enterprise force structure
e-mail	electronic mail
ESS	enterprise seed server
EwID	enterprise-wide identifier
GFM	global force management
GFM DI	Global Force Management Data Initiative
GFMID	global force management identifier
IT	information technology
OE	organizational element
OPR	office of primary responsibility
org	organization
OUID	organization unique identifier
PAS	personnel accounting symbol
POC	point of contact
RUC	reporting unit code
UDDI	universal description, discovery, and integration
UIC	unit identification code
UID	unique identification
URI	uniform resource identifier
URL	uniform resource locator
URN	uniform resource name
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
XSD	extensible markup language schema definition

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this volume.

TERM	DEFINITION
active seed	Within the ESS, the status of a given seed that denotes it has been assigned to a specific seed account holder. Within a tracker, the status of a given seed that denotes it has been used by a concatenator to generate 64-bit identifiers or else that it has been redirected to a subordinate tracker service.
ADS	Defined in DoDI 8320.03.
assigned seed	A seed that was provided to an OPR from the ESS administrator. The seed may be active or inactive.
concatenator	A device that combines a 32-bit seed prefix value obtained from the ESS with locally managed 32-bit suffixes to create 64-bit identifiers that are unique to the enterprise of ESS users.
EFS	Defined in DoDI 8260.03.
entity	A generic term for a data object with a distinct and independent existence.
ESS	The authoritative source of EwID seed values, on which seed users, or their intermediaries, must have an account. More information is located on the GFM DI ESS Website.
ESS user account	A formal relationship that allows an ESS user to create one or more seed accounts.
EwID	A scheme to generate unique identifiers that includes both a centralized and decentralized component. A prefix is provided by a centralized source to ensure enterprise-wide uniqueness, and a locally controlled suffix extends the procedure to distributed users. An EwID conveys no information about the entity it identifies, is a fixed 64-bit size, and is exchanged as a single attribute.
force structure	Defined in DoDI 8260.03.
generalization hierarchy	A structure grouping of entities that share common attributes, in which the most general or abstract concept is a super-type that is further specified by sub-type entities.

TERM	DEFINITION
generation	The act of concatenating a 32-bit prefix (seed) provided from a centrally managed source with a locally managed 32-bit suffix to create a full 64-bit GFMID.
GFMID	The set of EwID-based identifiers used to identify EFS data created using the GFM XSD. Based upon the EwID schema, GFMIDs convey no information about the entity they identify, are a fixed size of 64-bits, and are exchanged as a single attribute.
inactive seed	The status of an assigned seed that has never been used to generate a GFMID. This status is used to manage the GFMID tracking process at GFMID tracking servers. An inactive seed may be revoked back to the source from which it was immediately obtained.
joint	Defined in the DoD Dictionary of Military and Associated Terms.
node	Defined in Volume 2 of this manual.
org server	Defined in Volume 2 of this manual.
OUID	The means of uniquely distinguishing one DoD OE from another, allowing DoD systems to identify an organization individually across the DoD enterprise.
redirect/redirection	The act of delegating responsibility for a seed to an alternative server as a seed passes through multiple concatenators prior to full GFMID generation. The ultimate user of a redirected seed will thus not be identified in the ESS as the EwID account holder of that seed. The end user must therefore be identified through sequences of tracking services of every server through which the seed was redirected.
revoke	In GFMID management, the act of removing a seed that has never been used from the list of EwID seeds assigned to a user to be given back to the server from which it was originally received. This removes the seed from that end user's seed account.
seed	The 32-bit prefix used to generate a 64-bit identifier via concatenation with a 32-bit suffix.
sub-type	Within a generalization hierarchy, an entity that further refines the concept embodied by a super-type entity.
super-type	The uppermost entity of a generalization hierarchy, embodying a concept further refined by sub-type entities.

TERM	DEFINITION
tracking	The act of returning information about a given GFMID. This might be specific data referenced by the GFMID or a source for further querying (e.g., POC data or a web address).
UID	Defined in DoDI 8320.03.
UID standard	Defined in DoDI 8320.03.
unique identifier	Defined in DoDI 8320.03.
unit	An aggregation of separately identified OEs, and not as a unified entity such as occurs with a UIC.
URN	A string of characteristics that identifies a particular Internet resource that can span many networks and be mapped to different URLs in each network's UDDI registry.

REFERENCES

DoD Directive 5124.10, "Assistant Secretary of Defense for Manpower and Reserve Affairs (ASD(M&RA))," March 14, 2018

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Instruction 4165.14, "Real Property Inventory (RPI) and Forecasting," January 17, 2014, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 8260.03, "The Global Force Management Data Initiative (GFM DI)," February 19, 2014, as amended

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013, as amended

DoD Instruction 8320.03, "Unique Identification (UID) Standards for Supporting the DoD Information Enterprise," November 4, 2015, as amended

DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," September 3, 2015, as amended

DoD Instruction 8320.06, "Organization Unique Identification (OUID) Standards for Unique Identification of External Department of Defense Business Partners," September 26, 2012, as amended

DoD Manual 8260.03, Volume 2, "Global Force Management Data Initiative (GFM DI) Implementation: Unique Identification (UID) for GFM," November 20, 2009

Global Force Management Data Initiative Configuration Control Board Intellipedia Site, "Global Force Management Data Initiative/CCB"

Global Force Management Data Initiative Enterprise Seed Server Intellipedia Site, "Global Force Management Data Initiative/ESS"

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

United States Code, Title 10