

**FUNCTIONAL REQUIREMENTS DOCUMENT (FRD)  
FOR  
DEPARTMENT OF DEFENSE (DOD)  
ACTIVITY ADDRESS DIRECTORY/FILE (DODAAD/DODAAF)  
REENGINEERING EFFORT REQUIREMENTS STATEMENT**

**October 2003**

---

**JAMES A. JOHNSON**  
**Director**  
**Defense Logistics Management Standards Office**

## Table of Contents

<b>1. <u>General Description of Operational Capability</u></b>	<b>4</b>
a. Summary of Mission Needs	4
b. Overall Mission Area	5
c. Proposed IT Capability	5
d. System Mission	7
e. Operation and Support Concept	7
<b>2. <u>Threat</u></b>	<b>8</b>
<b>3. <u>Shortcomings of Existing Services</u></b>	<b>9</b>
<b>4. <u>Capabilities Required for Reengineering the DODAAD/DODAAF</u></b>	<b>11</b>
a. Solution Performance	11
b. Information Exchange Support Requirements	12
c. Logistics and Readiness	13
d. Other Systems Solution Characteristics	13
<b>5. <u>Functional Requirements</u></b>	<b>13</b>
a. System Access Requirements	15
b. Database Design Requirements	16
c. Database Update Requirements	18
d. Data Requirements	18
e. Database Inquiry and Download Requirements	18
f. Application Inquiry Requirements	19
<b>6. <u>Program Support</u></b>	<b>19</b>
a. Maintenance Planning	20
b. Support Equipment	20
c. D4I/Standardization, Interoperability, and Commonality	20
d. Computer Resources	20
e. Human Systems Integration (HIS)	20
f. Other Logistics and Facilities Considerations	20
g. Transportation and Basing	20

h. Geospatial Information and Services.....	21
i. Natural Environmental Support.....	21
<b>7. <u>Force Structure</u>.....</b>	<b>21</b>
<b>8. <u>Schedule</u>.....</b>	<b>21</b>
<b>Appendix A: <u>Schedule</u>.....</b>	<b>22</b>
<b>Appendix B: <u>New or Expanded Data Element Requirements</u>.....</b>	<b>22</b>
<b>Appendix C: <u>Abbreviations and Acronyms</u>.....</b>	<b>24</b>
<b>Appendix D: Drop Down Menu Choices for Data Entry</b>	

## **Figures**

Figure 1: Proposed DODAAD/DODAAF Architecture.....	6
Figure 2: Current DODAAD/DODAAF Architecture.....	9
Figure 3: Current DODAAD/DODAAF Architecture.....	10
Figure 4: Key Performance Parameters.....	10

## **1. General Description of Operational Capability**

### **a. Summary of Mission Needs**

The present DODAAD/DODAAF was designed using 1960's technology and has remained basically unchanged since its inception. New more capable methods are now available that must be evaluated and implemented to move the DODAAD/DODAAF process into the twenty-first century. This Functional Requirements Document (FRD) provides the preliminary requirements for reengineering and integrating the DODAAD/DODAAF, a key DOD reference repository. This is a two part effort with Phase I addressing improvements in support of the Defense Logistics Agency (DLA) and Phase II covering the remainder of DOD and other participating agencies.

Numerous audits have been highly critical of the DODAAD/DODAAF process. Criticisms of the DODAAD/DODAAF process include:

- 1) Architectural deficiencies include:
  - a) Batch transactional updates vice web-based real-time
  - b) Authoritative source file lacks data elements in Component files
  - c) Does not allow authoritative file to automatically update dispersed local copies
- 2) DOD Component service points do not validate and reconcile their files with the Defense Automatic Addressing System Center (DAASC)
- 3) DOD Component files have DOD Activity Address Codes (DODAACs) not in the Defense Automatic Addressing System(DAAS) master file
- 4) Present process allows unauthorized requisitioning
- 5) Some DOD activities obtained excess property using invalid DODAACs
- 6) Some DOD Components establish and maintain their own DODAAFs

To achieve the goals of the DLA Integrated Data Environment and DOD logistics, the architecture, management, and accessibility to key reference repositories must be reengineered.

### **b. Overall Mission Area**

The DODAAF contains addressing and other information about DOD activities that is needed by application programs and systems. The DODAAC serves as a reference code in the DODAAF which provides in the clear, machine-readable addressing information on activities that acquire material from the National Supply System (NSS) and for DOD activities that are NSS suppliers. DODAACs are assigned to provide the acquisition, logistics, and financial communities with a shorthand coded address for requisitioning, receipt, storage, issue, shipment, maintenance, and billing for materiel, supplies, and services.

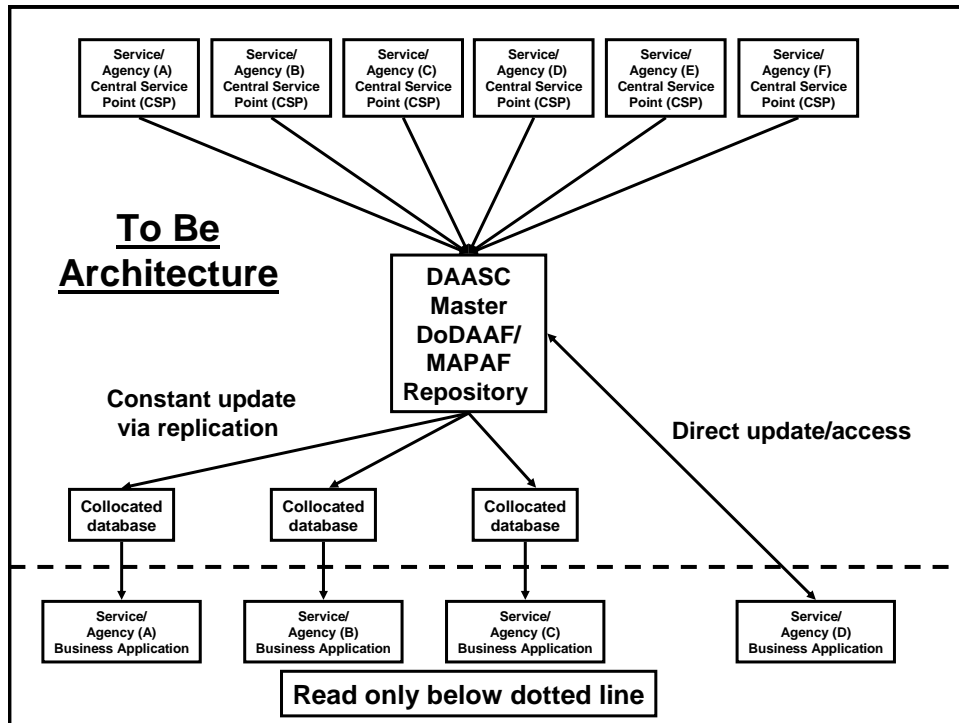
In addition to the basic addressing and routing function, the DODAAC carries a significant level of embedded intelligence. This embedded intelligence permeates the logic in DOD logistics systems. In addition to the basic addressing function it serves as:

- 1) An edit of incoming requisitions to validate the request is coming from an authorized user. The DODAAC acts as a password in this capacity and rejects invalid DODAACs.
- 2) A business rule key, application programs key on the DODAAC in part, in total, or in combination with other codes to select appropriate business rules to be applied to a particular function to be performed.
- 3) A tracking and interrogation key, by itself and as a sub-element of larger identifiers, like the document number and transportation control number. It is used extensively as a key for tracking the status of customer requisitions and location of requested materiel from the time of request to point of delivery. The DODAAC is key to obtaining current status and historical information for analysis in logistics systems.
- 4) A method to summarize and aggregate logistics information into different categories.

### **c. Proposed Information Technology (IT) Capability**

The proposed DODAAD/DODAAF architecture, illustrated at Figure 1, provides an integrated and centrally managed repository. The DOD Component Central Service Points (CSPs) will update the DODAAD/DODAAF authoritative source reference repository maintained by DAASC utilizing standard World Wide Web (www) technology. The Defense Logistics Management Standards Office (DLMSO) will specify the business rules and data standards and DAASC will execute them to include validation of CSP input. CSP input will be validated real time; if a data element fails validation the transaction will not get past the CSP user input screen until the entry is correct.

**Figure 1 – Proposed DODAAD/DODAAF Architecture**



The DAASC maintained authoritative source DODAAF will contain data elements that are currently in the DODAAD/ DODAAF plus those that have been included in the newly established DOD Trading Partner Number (TPN) file as well as those being used by the DOD Components for their own specific purposes. Once the update is complete, the new information will automatically update remote DODAAD/ DODAAF servers utilizing standard automated synchronization tools. The DAASC master repository will be the authoritative data source; replicate files will be kept in synchronization with the master. Replicates will only be updated via the DAASC master file. The replicate files will be read only, eliminating the need for file reconciliations.

Component applications will have the option of accessing remote servers or directly accessing the DAASC authoritative source repository server. Remote servers would be located at key DOD logistic facilities such that critical DOD logistics applications can query the database without traversing long haul communications. In addition, they can be provided with backup server addresses in the event of an emergency. These servers would be owned and maintained by DAASC and be located behind the facilities' firewalls connected to their local area network and would run no other applications other than those that support the DODAAD/DODAAF server software. DAASC would be responsible for monitoring and maintaining these remote servers. CSPs will no longer need their own Component specific DODAAD/DODAAF databases since updates would be applied directly to the DAASC authoritative source. The DOD Components will

no longer need to create and maintain their own DODAAD/DODAAF unique data elements. Benefits of the proposed architecture are:

- 1) Provides real-time www CSP DODAAD/DODAAC updates.
- 2) Ensures DAASC real-time validations and eliminates erroneous data.
- 3) Ensures automated file synchronization process and eliminates reconciliations.
- 4) Provides easy addition of the DOD Component unique data elements.
- 5) Provides Component applications near real-time access to the authoritative source data.

#### **d. System Mission**

The DLMSO is responsible for the developing and maintaining the business rules and data standards associated with the DODAACs and Activity Address Codes (AACs). The use of the DODAAC is prescribed in DOD 4140.1-R, DOD Materiel Management Regulation. Under the authority of DOD 4140.1-R, DOD 4000.25-6-M (for DODAAC and AAC) provides the uniform methods, codes, formats, and standards for the establishment, maintenance, publication, and dissemination of address data to requiring DOD Components, Federal Agencies, civil agencies, foreign governments and contractors.

DAASC is the central control point for the Federal Government and the authoritative reference repository for DODAACs and AACs. The DAASC mission is to receive, edit, translate, route and archive DOD logistics transactions.

#### **e. Operation and Support Concept**

The reengineered DODAAD/DODAAF shall continue to be administered by DLMSO with DAASC as the database custodian and operator. The DODAAD/DODAAF will operate in the future DLA and DOD logistics information environments, leveraging the current, and implementing future, data and service capabilities.

The DLMSO, with DAASC and the DOD Components, shall oversee, expand, and operate the DODAAD/DODAAF using appropriate Government or contract support resources. DAASC shall develop, operate, and maintain the DODAAD/DODAAF, maintaining central design activity. The infrastructure needed to support the DODAAD/DODAAF shall adhere to published DLA technology solution guidelines and DOD technical architecture mandates. The

supporting infrastructure includes the installed base of hardware, software, telecommunications, and security solutions; plus additional DAASC managed and maintained remote servers and software upgraded to meet revised architectural requirements. Due to the additional data elements in the reengineered file, the security classification of the file will be reevaluated.

## **2. Threat**

The vast amount of information stored, processed, and transferred by these systems makes them a lucrative target of a diverse worldwide threat intent on compromising and corrupting data, disrupting service or destroying the actual physical system. The threat is diverse in source, motivation, sophistication, technique, and time. It includes hackers fascinated by technical challenge, foreign governments motivated by military and economic interests, disgruntled employees, and inadvertent software errors. While the threat is predominantly in the operational phase of the system life cycle, it is present throughout system development and sustainment. Threats to the DODAAD/DODAAF are the threats that apply to any DOD logistics data integration capability with its associated communications infrastructure. Standard threats applicable to DODAAD/DODAAF are:

- a. Natural disasters** such as fire, earthquakes, and floods.
- b. Accidental acts** such as electrical power interruption and operator or user error.
- c. Intentional acts** such as bomb threats, sabotage, theft, and vandalism.
- d. Acts of war** such as information operations and the destruction of a facility, terminal, or satellite through deliberate enemy attack.
- e. Security threats** such as unauthorized users, viruses, back doors, and authorized users who modify the program in unauthorized ways.
- f. Electronic warfare** that attacks the communication system with which the DODAAD/DODAAF must interface. Electronic warfare includes, but is not limited to, jamming, intrusion, message interception, and traffic flow analysis.

DLA has conducted a detailed threat assessment in order to determine specific threats associated with each broad threat category presented above. Appropriate countermeasures have been selected to mitigate those threats.

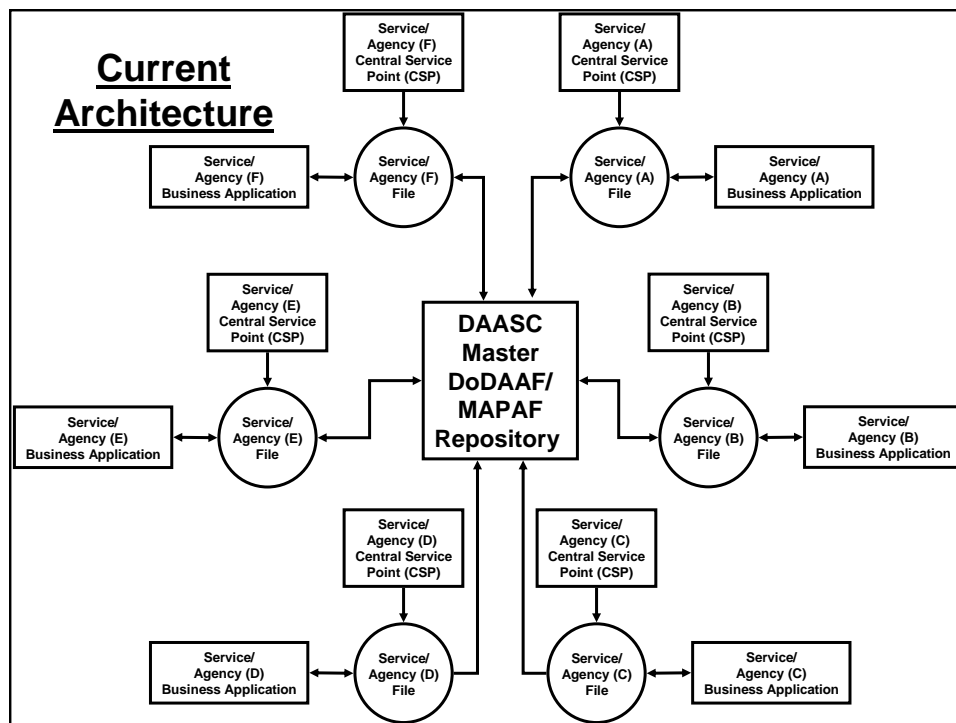
## **3. Shortcomings of Existing Services**



Figure 2, below, is a simplistic graphic depicting the current DODAAD/DODAAF architecture. The DODAAD/DODAAF consists of approximately 30 CSPs. The CSPs are responsible for keeping the DODAAD/DODAAF up-to-date for their respective Component. Since the DODAAD/ DODAAF repository and the legacy systems it supports were developed in the 1960s, long before the www and the robust communications that exists today, each application requiring DODAAD/DODAAF information usually has a local copy, collocated with the application. CSPs update local copies via an update program, which, at some point, sends the updated transactions to DAASC where the authoritative repository is maintained. In some cases, the CSP updates both the local file and the DAASC file simultaneously. However, in both cases, there is no assurance the edits and timing of the updates of the local and DAASC authoritative source files are done such that the file(s) content are synchronized.

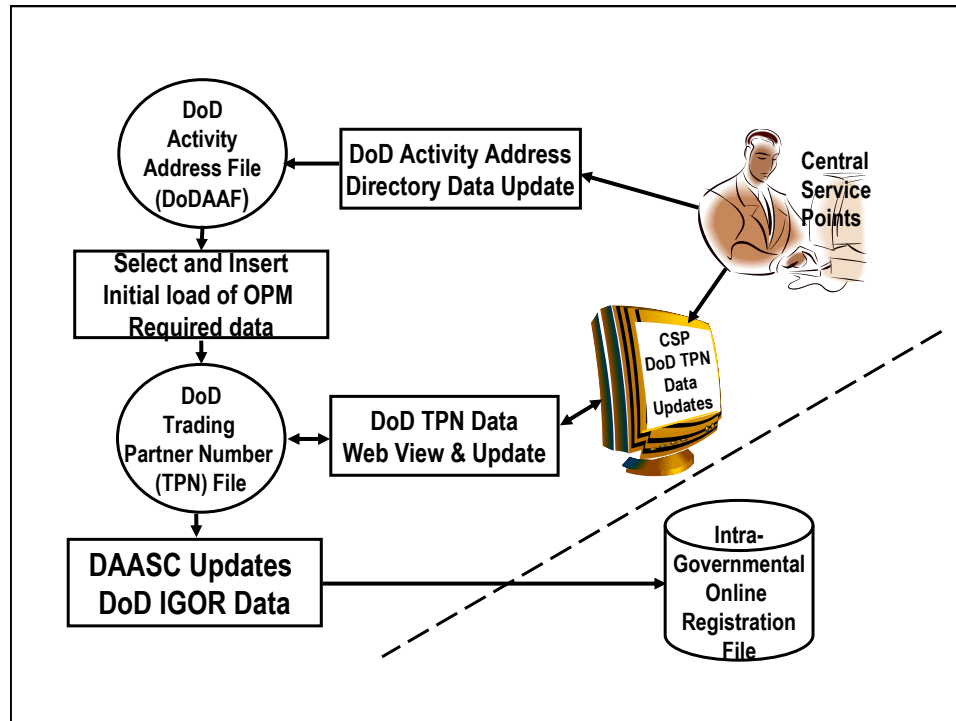
To ensure local and authoritative source files are synchronized, periodic reconciliations of the files are conducted. Reconciliations are mechanical matches of the DAASC authoritative source file to the copy(s), discrepancies are identified and corrections are made to bring files into agreement. This ineffective process that is conducted infrequently, and even when completed, it only ensures that the authoritative source file and the reconciled copies are in agreement at a moment in time. Anytime the files are not in agreement, the potential exists for one or more applications to either not process an operational transaction (requisition, return, lateral transfer, etc.) at all, or process it incorrectly.

**Figure 2 – Current DODAAD/DODAAF Architecture**



A recent requirement to register DOD buying and selling activities within the Business Partner Network (BPN) necessitated the creation of the DOD Trading Partner Number (TPN) File which feeds the BPN with data on DOD activities. In the interest of expediency and to minimize the impact on DOD legacy application systems that utilize the DODAAD, a separate DOD TPN file was implemented. The TPN files base data is provided by the DODAAD but a separate Web update capability was implemented to allow CSPs to add the data that is required to support the BPN requirements. While this approach was expedient to meet the BPN implementation schedule, it further complicated the existing architecture, adding yet another file requiring synchronization, and it requires that the CSPs take two separate actions to ensure that all the necessary data updated. Figure 3 shows the high level architecture with the addition of the TPN requirement.

**Figure 3 – Current DODAAD/DODAAF Architecture Including the TPN Requirement**



Principal deficiencies of the current architecture are:

- a. **Discrepancies between** the DAASC authoritative source file and Component collocated copies result in delayed or erroneous processing of operational logistics transactions.
- b. **Authoritative source file** does not contain all data Components have appended to their locally maintained DODAAD/DODAAF files.

- c. **Two separate updates are required** to add a new DODAAC. The Basic DODAAD directory must be updated with the new DODAAC using the current transaction update methodology and then the additional information related to the intragovernmental transactions DOD Trading Partner Number (TPN) must be updated separately using the DOD TPN Web update.
- d. **Near zero latency access** to the DAASC authoritative source file to support local applications is not allowed, nor does it capitalize on existing technology that allows authoritative sources to automatically update dispersed local copies.

#### 4. **Capabilities Required for Reengineering the DODAAD/DODAAF**

##### a. **Solution Performance**

- 1) **Key Performance Parameters.** DAASC is the central repository for the DODAAD/DODAAF and is responsible for managing and operating the repository. The Component CSPs or their designated agents are the authoritative sources for data input and quality. Under this proposed architecture, the DLMSO produced business rules and the DAASC developed edits shall ensure the DOD Components input data that is reliable, accurate, and timely. The established file is being expanded to support the DOD Component internal justified data needs in addition to DOD and other Federal Agency requirements including those of the intragovernmental transactions. This will eliminate the need for duplicative files.

**Figure 4 – Key Performance Parameters**

Key Performance Parameters	Top-Level Metrics	Threshold	Objective
Interoperability	Facilitate seamless integration within DLA and DOD, and with commercial trading partners by implementation of interfaces to support information and data exchange	98 percent successful electronic data exchanges	100 percent successful electronic data exchanges
Availability	Percentage of the time the DODAAF capability is available for use, excluding scheduled downtime	Provide access and connectivity at a 98 percent success rate to authorized subscribers	Provide access and connectivity at a 100 percent success rate to authorized subscribers

Key Performance Parameters	Top-Level Metrics	Threshold	Objective
Reliability	24-hour per day operations with maximum data integrity, minimal site failures, minimal recovery times, and maximum availability of guaranteed backup	98 percent reliability	100 percent reliability
Timeliness	Retrieval and provision of current data from the DODAAF in near real-time.	Application programs retrieval <1 second. Web query retrieval <3 second (dependent on customer constraints)	Application programs retrieval near real-time. Web query retrieval <1second (dependent on customer constraints)
Relevancy	Provide accurate data from authoritative sources as determined by established business processes.	98 percent of all data exchanges. DOD Component CSPs are responsible for data accuracy	100 percent of all data exchanges. DOD Component CSPs are responsible for data accuracy
Security	Ensure data security and integrity by complying with all applicable DOD Security regulations and directives for classified, sensitive but unclassified, and unclassified information	100 percent of standard	100 percent of standard

2) Key Functional Requirements. The benefits to be derived from this reengineering effort are listed in section 1.c.1 through 5, above. Realizing these benefits will lead to the attainment of the following key functional requirements outcomes:

- a) Increased data accuracy
- b) Simplified access to data by authorized users
- c) Faster updates to the DODAAF
- d) Elimination of duplicate updates and files
- e) Increased support to multiple business processes
- f) Utilization of eBusiness/eCommerce business practices and tools
- g) Supports DLA and other DOD Component modernization efforts

#### **b. Information Exchange Support Requirements**

1) DLA DODAAD/DODAAF Users:

- a) Defense Distribution Center (DDC)
- b) Defense Supply Center Richmond (DSCR)
- c) Defense Supply Center Columbus (DSCC)

d) Defense Supply Center Philadelphia (DSCP)

e) Any authorized user making a DODAAD Web query.

(NOTE: Other DOD and non-DOD users will be identified and added under Phase II.)

- 2) Proposed Future Operational Architecture. See section 1.c, above.
- 3) Business Systems Modernization (BSM) and Distribution Standard System (DSS) Interface Support. Modernization of the DODAAD/DODAAF process will provide BSM and DSS with an up to date process that will increase their capability to support the war fighter.
- 4) DLA Internal Interface Support. In addition to the BSM & DSS interface support; this effort will have a direct benefit to the DLA Supply Centers, the Defense Distribution Center and the supply distribution depots. The DODAAC is critical to DOD logistics and transportation processes. It is used as a validation/security check, for determination of the appropriate business rules to be executed, for tracking and interrogation, for summarization/aggregation, and for assignment of the correct address for the particular application situation. The modernization of the DODAAD/DODAAF process will directly benefit the Centers and the customers they support.
- 5) Program Top-Level Operational Architecture diagram – N/A
- 6) Program Top-Level System Architecture diagram – N/A

**c. Logistics and Readiness – N/A**

**d. Other Systems Solution Characteristics – N/A**

## **5. Functional Requirements**

This section provides the functional requirements for the reengineered DODAAF/DODAAD.

- a. System Access Requirements.** The following provides a summary of the requirements to access the system.

1. There will be multiple levels of access governed by the roles of the user. The DLMSO DODAAD Administrator will set the access governing policy and the DAASC DODAAD System Administrator will maintain the access controls to the system. All access will be user ID and password controlled. The system will accommodate DOD Public Key Infrastructure (PKI) requirements.
2. The system will provide a WEB screen from which potential users can request access. This Screen will request information regarding the type of access required (drop down list), information about the requestor (fill in the blanks), need for access (drop down), component affiliation (drop down), and request that they enter and verify their desired password (fill in blanks).
3. All access permission requests, except the General Access level, will be forwarded via email to both the DLMSO DODAAD Administrator and the DAASC DODAAD System Administrator for approval. Upon approval the system will send an email back to the requestor notifying them of the approval and providing them their user ID.
4. The system will grant immediate approval to General Access requesters, however it will still notify via email the DLMSO DODAAD Administrator and the DAASC DODAAD System Administrator that access has been granted, providing the information on the requestor.
5. The system will provide a database profile of all users with access by access level and it will maintain statistics on the number of accesses and types of access (update, query, download) by user. The system will maintain data on attempted unauthorized accesses and notify the DLMSO DODAAD Administrator and the DAASC DODAAD System Administrator via email.
6. The access levels and the authorities each has will be as follows:
  - a. **The System Administration Level:** This highest level of access, it will be granted to the DLMSO DODAAD Administrator and the DAASC DODAAD System Administrator. They will have access to all data and will be able to download any information in the data base. They will also have access to all user profiles and usage data.
  - b. **The Component Central Service Point Level:** This level will be granted to the individual designated by each DOD Component as their Central Service Point (CSP). Each Component will designate their CSP to the DLMSO DODAAD Administrator who will notify the DAASC DODAAD System Administrator. The user ID will be structured such that, when a CSP logs into the system, the system recognizes the CSP and the DODAACs and related information for which that CSP has responsibility. The CSP will have the ability to access all information in the

database and can update any information for the Component for which they have responsibility. A CSP will not be able to update information on other Component DODAACs, i.e., the Army CSP will not be able to update Navy DODAACs or the information related to them. The CSP will also have access to all data relating to the user profiles and usage data for the users affiliated with the Component for which they are responsible.

c. **Component Central Service Point Administration**

**Level:** Component Level CSPs can delegate/sub-divide their responsibility for file maintenance of the DODAACs for which they are responsible. A maximum of 20 delegations per CSP are allowed. Each CSP must identify to the DLMSO DODAAD Administrator and the DAASC DODAAD System Administrator the individuals to whom sub-delegations are being made and the DODAACs that each is responsible for. The user ID will be structured such that, when a CSP Administrator logs into the system, the system recognizes the CSP Administrator and the DODAACs and related information for which that CSP Administrator has responsibility. The CSP Administrator will have the ability to access all information in the database and can update any information for the Component for which they have been assigned responsibility by their CSP. A CSP Administrator will not be able to update information on other Component DODAACs, or DODAACs assigned to another CSP Administrator within their Component.

d. **General Access Level:** This level provides user access to view any general information in the database via the query program. Downloads of the database information will be controlled by the DLMSO DODAAD Administrator and the DAASC DODAAD System Administrator.

e. **Application Access Level:** This level is the Component business application level access to the data base, applications will have no ability to change the database but will have unlimited access to the data. The initial business application access arrangements will be made by the DAASC DODAAD System Administrator in consult with the DLMSO DODAAD Administrator.

b. **Database Design Requirements.** The following provides an overview of the database design requirements for the system.

1. The database design structure priority will be to maximize Component business application access speed. The DODAAC will

be the principal key for business application accesses to the DODAAD database.

2. The database/system design shall be such that Web based access inquiries or downloads are responsive to Web users with no degradation of the responsiveness to Component application accesses.
3. The master DODAAD database will reside at DAASC with physical copies at both the Dayton and Tracy sites. The two copies of the master database will be kept in constant synchronization.
4. Application accesses and Web user inquiries will be balanced among the two sites to maximize responsiveness.
5. The master database will always be available; if one of the two physical sites is down for any reason the other site will pick up the accesses and Web queries until full service is restored. When necessary Web access query responsiveness will be degraded or suspended to ensure maximum responsiveness to application accesses.
6. The master database will only be updated via the DODAAD Web update or via mass update discussed in the Database Update Requirements Section below.
7. Local copies of the database will be provided (to include hardware and software as required) by DAASC to applications with critical high volume access requirements, such as the Distribution Standard System. These local data base copies will be collocated with the using application requiring access and they will be kept in constant synchronization with the master copies maintained at DAASC. All changes to the local databases will be controlled by the master DODAAD database.
8. The database will be segmented to accommodate data that is common across the Components (DOD-wide data elements) and data that is common to one Component but not the others (Component unique data).
9. The initial database will provide for all the data identified in the System Data Requirements Section.
10. The database will be designed to easily accommodate expansion for new data elements (both DOD-wide and Component unique) as future requirements dictate.

**c. Database Update Requirements.** The following provides the requirements for updating the system database.

1. The database shall be updated only via the Web update program by the CSP or authorized designee. Requirements for mass database updates, should they be required, will be accomplished by identifying the requirement to the DLMSO



DODAAD Administrator and the DAASC DODAAD System Administrator.

2. Full on-line editing shall be provided making maximum use of drop down menus. Individual data element edit criteria shall be in accordance with Appendix \_\_\_\_.
3. Data entries will be validated in accordance with Appendix B criteria, on screen identification of invalid data will be presented, and the master database will not be updated until all the data passes validation.
4. The Component CSP or their designated CSP administrator is the sole authoritative source for all input data associated with the DODAACs for which they are responsible.
5. There shall be a Web update page(s) for all the DOD-wide data elements; this shall be the first page(s) to come up after logging onto the Web update. This page(s) shall be the same for all users having update capability, which is determined by the system access requirements.
6. There shall be separate Web update pages for the Component unique data; the appropriate page shall be determined by the user ID at time of login (Army page for Army CSP or designated Army CSP Administrator(s), DLA CSP or designated CSP Administrator(s), etc).
7. The authoritative input source shall have the ability to specify, via drop down, an effective date for submitted changes. This capability shall allow the submitter to specify a single future effective date all changes made during the update session or to specify that the changes made to the data entries for a single DODAAC take effect on a future specified effective date. This will be accomplished via a drop down menu choosing immediate update or by choosing a date from a drop down calendar. When no effective date is specified the system will effect the update changes immediately.
8. DODAACs that are being deleted shall be flagged and retained in the database as active for five years. This will allow time for all transactions to clear the pipeline. Any new requisitions using deleted DODAACs during this active period shall be rejected. The five year retention period will begin on the date the DODAAC is flagged as deleted; i.e., if the user specifies a future effective date (item 6 above), the three years begins as of that date. At the end of the three years the retired DODAACs and all the associated data will be removed from the active database and moved to a retired DODAACs database.
8. When establishing new DODAACs or changing the address information the authoritative submitter shall always enter address data for the Type Activity Code (TAC) 1 address (Postal Address), but for TAC 2 addresses freight or

commercial small parcel address) and TAC 3 (bill to mailing address), the user shall have a drop down option of choosing “Same as TAC 1, YES, or NO ”. If “Yes” is chosen, the system shall duplicate all the address information for the TAC 2. If “NO” is chosen then the user shall be offered another choice “Is Address that of another DODAAC Yes or No,” if “Yes” then a block shall be presented to fill in the desired DODAAC and the system shall populate the TAC 2 address for the DODAAC undergoing change with the TAC 2 addressing information of the DODAAC entered. If “No”, then blank addressing blocks shall be presented to the user to enter the addressing information in the spaces provided. The TAC 3 shall have the same option provided. If the TAC 1 address is a Post Office Box then there must be a different TAC 2 address suitable for shipping materiel.

9. Provision will be made for TAC 4 address updates. A TAC 4 address will reflect a commercial small parcel address. TAC 4 addresses are optional entries.

**d. Data Requirements.** The specific data elements and their related information are found in Appendix B.

**e. Database Inquiry and Download Requirements.** The following summarizes the database inquiry and download requirements, to include a wildcard capability. This capability may be limited to first 300 records.

1. All Web originated inquiries will be processed against the DAASC master database.
2. The Web inquiry will provide for inquiry by any one or combination of the following fields.
  - City
  - DODAAC
  - CommRI (status and billing)
  - Distribution Code
  - RIC
  - Zip Code
  - Address Type – (TAC 1, 2, 3 or 4)
  - Service/Agency drop down name list
  - Address Line(s) (1, 2, 3, or 4)
  - WP
  - AP
  - Break Bulk Point
  - Consolidation and Containerization Point drop down
  - Standard Point Location Code

Command/Bureau code **drop down**

State/province code **drop down**

Country **drop down**

CONUS/OCONUS **drop down**

Navy TAC 3, DODAAC Fiscal Station Number (FSN)  
(AAA) (ADSN)

UIC

Authority Code **drop down**

Service **drop down**

Effective Date Ranges

3. Search selections fall into two categories: drop downs lists and free form search:

- a. The drop down lists should be used for any “code” lookup, where a free form search would not be appropriate. For example, the State codes would use a drop down list. The user would select the state by name (e.g., Maryland) and the query would use to appropriate code (e.g., MD).
- b. Free form searches need an additional qualification to define how the search is to be used. Below is a list of how the searches should be qualified and performed.

DODAAC

**Begins with** – this is a wild card search with the match performed on the left most characters entered. For example, if the user enters “123” the resulting search would return all DoDAACs that begin with “123” (e.g., select \* from table where dodaac like ‘123%’)

**Contains** – this is a wild card search with the match performed on both sides of the characters enters. For example, if the user enters “123” the resulting search would return all DoDAACs that have “123” any where in the string (e.g., select \* from table where dodaac like ‘%123%’)

**Ends with** – this is a wild card search with the match performed on the right most characters entered. For example, if the user enters “123” the resulting search would return all DoDAACs that end with “123” (e.g., select \* from table where dodaac like ‘%123’)

**Is** – this is an exact match or ‘equal to’ search. Whatever is entered must equal the value in the table. For example, if the user enters “12345” the resulting search would only return the DoDAAC “12345” (e.g., select \* from table where dodaac = ‘12345’)

**Is not** – this is a non-match or ‘not equal to’ search. Whatever is entered is excluded from the table search. For example, if the user enters “12345” the resulting search would return all

DoDAACs that are not equal to “12345” (e.g., select \* from table where dodaac <> ‘12345’)

**Is blank** – this is null value search. No value is entered and the table is searched for blanks or missing values in the table search (e.g., select \* from table where dodaac is null). *This search is only appropriate in certain cases, and is meaningless if the field is required.*

**Is not blank** – this is an ‘any value’ search. No value is entered and the table is searched for any valid value found in the field selected in the table search (e.g., select \* from table where dodaac is not null). *This search is only appropriate in certain cases, and is meaningless if the field is required.*

**Between** – this is a special type of search for dates, so a range of dates can be entered. The generated query will search for dates between the values entered in the table search (e.g., select \* from table where EffectiveDate between ‘2006-01-01’ and ‘2006-12-31’)

4. Outputs – there should be two types of outputs for query results: Excel and HTML.

- a. Excel display all elements (TAC 1, 2, 3, and 4), broken out by DoDAAC, with one DoDAAC per line.
- b. For the HTML output, the list should be limited to key information only, and you will need to click on a hot link to display the “complete” DoDAAC. Key information is: DoDAAC, Country, Address line 1, city, state, zip, and TAC type.
  - i. TAC should be part of the display list and only “found” information should be returned. For example, if the search query is searching for ‘MD’ in the state code field and ‘MD’ is only found in the TAC 2 area, only TAC2 information would be returned in the result list. From the query result list the user may click on a hot link in the result list if they want to see all information associated with that particular DoDAAC.

**f. Application Inquiry Requirements.** The system inquiry requirements for the application are provided in the following. The following provides a summary of the requirements to access the system.

1. Application systems will have read only access to either the DAASC master database or the database that DAASC maintains that is collocated with the application system. All application systems will have the capability to access the DAASC master

database even if their normal access is to a DAASC controlled collocated database. The source database for application inquiry (master at DAASC sites or collocated with application) will be determined on a case-by-case basis.

2. DAASC will continue to push data to legacy systems in the format that they currently accept until the legacy system is replaced, or is modified, or until 1 October 2006, which ever occurs first.
3. DAASC will continue to push data to the Business Partner Network in the current format indefinitely.

## **6. Program Support**

This section describes the program support objectives for the reengineered DODAAF/DODAAD.

### **a. Maintenance Planning**

- 1) Software maintenance. Software maintenance consists of creating, testing, and fielding software updates. The solution will maximize commercial off-the-shelf (COTS) software to the extent possible.
- 2) System Maintenance. Shall include installation of software maintenance releases, version releases, and remote help desk support. DAASC will update and maintain master repository as the authoritative data source of record. Replicated files will be updated by DAASC and kept in constant sync with the master.
- 3) Hardware Maintenance. Maintenance of DODAAF specific hardware will be maintained and improved by DAASC. These servers will be owned and maintained by DAASC.
- 4) Business process. DODAAD/DODAAF business rules and processes shall continue to be developed by DLMSO and implemented by DAASC, DLA, DOD Components, and participating agencies. All changes shall be implemented in a configuration-controlled environment.
- 5) Significant emerging requirements. The DODAAD/DODAAF reengineering shall take advantage of the latest COTS solutions to bring this process into the twenty-first century. The design shall be done so new technology methods can easily be applied without major redesign.

### **b. Support Equipment**

The reengineered DODAAD/DODAAF does not require any special support equipment. Remote servers will be purchased and owned by DAASC.

**c. D4I/Standardization, Interoperability, and Commonality – N/A**

**d. Computer Resources**

There are no computer resource constraints (i.e., language architecture, interoperability and database) on the reengineered DODAAD/DODAAF.

**e. Human Systems Integration (HSI)**

There are no physical HSI requirements.

**f. Other Logistics and Facilities Considerations**

There are no other logistics and facilities considerations.

**g. Transportation and Basing**

There are no requirements for transportation and basing.

**h. Geospatial Information and Services**

There are no requirements for geospatial information and services.

**i. Natural Environmental Support**

Natural environment support is not required.

**6. Force Structure**

Not applicable

**7. Schedule**

The schedule for Phase I of this project is found in the Plan of Action and Milestones (POA&M) in Appendix A.

## **Appendix A – Schedule (POA&M)**

1. Requirements Determination	
a. DLMSO/DAASC Meeting	05/06/03 2days
b. DLMSO/DAASC/DSIO-U/DDC/J-3	06/11/03 2 days
c. CSP/Component Meeting	07/29/03 2 days
d. Finalize requirements Doc/Staff	08/04/03 2 days
2. Configuration Management Working Group	08/26/03 2 days
3. DAASC/DLMSO Preliminary Design Review	10/23/03 1 day
4. Preliminary DSIO-U Design Review	11/18/03 2 days
5. Critical DISO-U Design Review	01/06/04 3 days
6. DLMSO/DAASC Final Design Review	02/13/04 1 day
7. Hardware installation complete for testing	03/03/04
8. DAASC/DSIO-U System Interface Test (File access is required at this point)	03/17/04 5 days
9. DAASC Programs completed and Tested	05/01/04
10. Training of CSPs completed	May 04
11. DODAAD Manual Redrafted.	May 04
12. IOC with DSS	June 04

## Appendix B – New or Expanded Data Element Requirements\*

Data Element Name	Size	Mandatory Optional	Validation	Source	Remarks
Country Code (For each TAC)	2 and 3 digit alpha	M	Drop down Menu	Table	ISO and MILS will be used
State/Province Code	2 digit alpha/or numeric	C	Drop down menu	Table	Mandatory for US And Canada
City	21 alpha/numeric				
Major Command/Bureau	2 digit alpha/numeric	M	Drop down menu	Service Input	
Standard Point Location Code (SPLC)	9 digit numeric	C	No validation	Web entry	CONUS – M All others - O
Zip Code	10 digit (5+4) numeric incl dash (-)	M		Table	Entering zip should populate the City & State Mandatory for CONUS
International Postal code	10 digit alpha/numeric				
Point of contact (POC) (generic)					
POC phone # - Commercial	21 digit numeric	M	No validation	Web entry	If not entered default to CSP
Name/title	24 alpha/numeric	O	No validation	Web entry	Service provided Default or CSP
POC email(generic)	40 digit alpha/numeric	M	No validation	Web entry	
Consolidation and Containerization Point (CCP)	3 digit numeric	O	Drop down menu		
Break Bulk Point	6 digit alpha/numeric	O	Validate DODAAC	Web Entry	TAC 1&2 will have separate BBPs
Ports: APOD and WPOD are mandatory for all OCONUS address and Hawaii, Guam Puerto, Guam.	APOD and WPOD are optional for CONUS and addresses on the CRIF				
Air port of embarkation	3 digit alpha/numeric	C	TBD	Web Entry	APOE will be deduced
Water port of embarkation	3 digit alpha/numeric	C	TBD	Web Entry	WPOE will be deduced
Air port of debarkation	3 digit alpha/numeric	C	TBD	Web Entry	APOD will be entered
Water port of debarkation	3 digit alpha/numeric	C	TBD	Web Entry	WPOD will be entered
Air Lines of Communication (ALOC)	1 digit numeric	O	TBD	Web Entry	
Contractor DODAAC Contract Number	17 digit alpha/	O	TBD	Web	



Contract expiration date	numeric 8 digit numeric	O	TBD	entry Web entry	Ccyymmdd
Contract Administration Office	6 digit alpha numeric	O	TBD	Web entry	
Cage Code	5 digit alpha/ numeric	M	TBD	Web entry	
Addressing format					
Line 1-Activity	35 digit alpha/numeric	M	None	Web entry	CONUS-To include Hawaii,Guam,PuertoRico And Canada
Line 2-Street Address	35 digit alpha/numeric	M	None	Web entry	
Line 3-POC name and number	35 digit alpha/numeric	O	None	Web entry	
Line 4-City, State, Province, Region Country and zip or postal code	35 digit alpha/numeric	M	None	Web entry	
Authority Code	2 digit	Drop down menu			
Routing Identifier Code (RIC)	3 digit alpha/ numeric	C	Table	Web entry	Based on authority code
CommRI					
Billing	7 digit alpha/	O	Table	Web entry	
Status	7 digit alpha/	O	Table	Web entry	
Latitude and Longitude	14 digit alpha/ numeric	O			Not published – DAASC looking into a tool to populate
Distribution Code	1 digit numeric	O	Drop down entry	Web entry	
Area of Responsibility	Up to 8 digit alpha	O	Drop down menu	Web entry	Indicates the unified command the DODAAC is assigned to (Combatant command) Required for issuers of Bill of LADINGS
Bill of Lading Code (BLOC)	4 digit alpha/ numeric	C		Web Entry	
<b>DATA ELEMENTS FOR TPN</b>					
Agency Name	Text field 100 characters alpha/numeric	M	No validation	Web entry	Based on D&B provided information.
Bureau Name	Text field 100 characters alpha/numeric	M	No validation	Web entry	Based on D&B provided information
DUNS	9 digit alpha numeric	M	No validation	Web entry	Numeric only for Civilian agencies alpha/numeric for DOD. Dun and Bradstreet defines number associated with the registering entity, Office or Division.
Employer Information Number (EIN)	9 digit numeric	M		Web	

Agency Location Code	8 digit numeric	M		entry Web entry	Agency location code that corresponds with DUNS number location. Used only when there are different ALC's for the same DUNS #(office). Not to be used to indicate different addresses. Agency defined.
DUNS + 4	4 digit numeric	O			Enter the Disbursing Office Code that corresponds with appropriation or ALC. Registration POC This is the person responsible for the data in the registration record.
Disbursing Office Symbol	5 digit alpha numeric	M		Web entry	Eliminations POC – The designated agency contact for financial statement eliminations. Will include a drop down list of previously registered contacts for that agency.
Points of Contract (two for each registering entity)					
First Name	Alpha 60 characters with special characters (apostrophe and hyphen)	M	No validation	Web entry	
Middle Initial	1 character alpha	O	No validation	Web entry	
Last Name	60 characters alpha with special characters (apostrophe and hyphen)	M	No validation	Web entry	
Email	100 characters alpha numeric with special characters @, period, hyphen underscore	M	No validation	Web entry	Must be the person's actual (direct)email.
Phone	30 digit numeric	M	No validation	Web entry	
Extension	6 digit numeric	O	No validation	Web	
Fax	30 digit numeric	O	No validation	Web entry	
Street Address Line 1	100 digit alpha/numeric No PO Box	M	No validation	Web entry	

Street Address Line 2	55 digit alpha/numeric. May have PO Box	M	No validation	Web entry	
City	35 digit alpha	M	No validation	Web entry	
Country	3 digit alpha	M			
State	2 digit alpha	M			
Zip	9 digit (5+4) alpha/ numeric	M			
Postal Code	35 digit alpha/ numeric	O	No validation	Web entry	Optional for foreign addresses. Can't contain USA ZIP codes.
Business Type	Text box with "Buying", "Selling", "Both Buying and Selling.	M	No validation	Web entry	Indicates if registering entity represents buying or selling agency, or both. If "Selling" or "Both Buying and Selling" is chosen, Seller fields are mandatory. If "Buying" or "Both Buying and Selling" is chosen, Buyer fields are mandatory.
Seller Information – The Following information need only be filled out by Sellers (including "Both Buyer and Seller)					
Annual Revenue	Numeric (no limit on length) no decimals, with special characters (commas)	M	No validation	Web entry	Total revenue from Intra-governmental sales for the previous fiscal year. Must be updated during annual validation.
Credit Card	1 digit alpha 0-No, 1-Yes	M	Drop down menu	Web entry	Indicate if Govt purchase card can be used for payment. Entered for information purposes only. If answer is Yes, Merchant ID is mandatory.
Merchant ID Number 1	Numeric- No limit on length	O	No validation	Web entry	Assigned by the Credit Card Processor. Mandatory if Credit Card answer is yes. If merchant ID number changes the new number should be entered over the old. The system will track old numbers.
Merchant ID Number 2	Numeric-No limit on length	O	No validation	Web entry	Used if registering entity has two routing numbers (uses both banks). If merchant ID number changes the new number should be entered over

Federal Supply Class (FSC)	4 digit alpha/numeric.	M				the old. The system will track old numbers. May specify up to 20 different codes. FSC code for products provided. Mandatory. Assists in determining what products/service the provider provides.
North American Industrial Classification (NAICS)	6 digit numeric	M				May specify up to 20 different codes. Describes type of goods and services sold.
Points of Contact (two for each selling entity)						Accounts Receivable POC –The contact for questions regarding billing. Should be generic phone, fax and email. Will include drop down list of previously registered contacts for that agency.
						Sales POC – The person who can provide information about what products and services are provided. Should be organization phone, fax and generic email. Will include a drop down list of previously registered contacts for that agency.
Name	60 digit alpha	M	No validation	Web entry		
Email	100 digit alpha numeric with special characters@, period, hyphen, underscore.	M	No validation	Web entry		Generic email
Phone	30 digit numeric	M	No validation	Web entry		
Extension	6 digit numeric	O	No validation	Web entry		
Fax	30 digit alpha numeric	O	No validation	Web entry		
Street Address Line 1	100 digit alpha/numeric – No PO Box	M	No validation	Web entry		
Street Address Line 2	Digit alpha Numeric May have PO Box	O	No validation	Web entry		
City	35 digit alpha	M	No validation	Web entry		
State	2 digit alpha	M				

Zip	9 digit (5+4) alpha/ numeric	M				
Postal Code	35 digit alpha/ numeric	O	No validation	Web entry	Optional for foreign addresses. Can't contain USA Zip code	
<p>Buyer Information – The following information need only be filled out by Buying entities (includes Both Buying and Selling)</p> <p>Point of Contact</p>						Accounts Payable POC – The contact for questions regarding a payment. Should be organization phone, fax and generic email. Will include a drop down list of previously registered contacts for that agency.
Name	60 digit alpha	M	No validation	Web entry		
Email	100 digit alpha numeric	M	No validation	Web entry	Generic email	
Phone	30 digit numeric	M	No validation	Web entry	30 if international	
Extension	6 digit numeric	O	No validation	Web entry		
Fax	30 digit numeric	O	No validation	Web entry		
Street Address Line 1	100 digit alpha numeric – No PO Box	M	No validation	Web entry		
Street Address Line 2	55 digit alpha numeric – May have PO Box	O	No validation	Web entry		
City	35 digit, alpha	M	No validation	Web entry		
State	2 digit alpha	M				
Zip	9 digit (5+4) alpha numeric	M				
Postal Code	35 digit alpha numeric	O	No validation	Web entry	Optional for foreign addresses	
<b>Service Unique Requirements</b>						
Air Force						
Geographic Zone	1 digit alpha numeric	M	Drop down menu	Web entry	See appendix D for codes	

## **Appendix C – Abbreviations and Acronyms**

AAC	Activity Address Code
BSM	Business System Modernization
COTS	Commercial Off The Shelf
CSP	Central Service Point
DAAS	Defense Automatic Addressing System
DAASC	Defense Automatic Addressing System Center
DDC	Defense Distribution Center
DISO	Defense Information Systems Office
DLA	Defense Logistics Agency
DLMSO	Defense Logistics Management Standards Office
DOD	Department of Defense
DODAAC	DOD Activity Address Code
DODAAD	DOD Activity Address Directory
DODAAF	DOD Activity Address File
DSCC	Defense Supply Center Columbus
DSCP	Defense Supply Center Philadelphia
DSCR	Defense Supply Center Richmond
DSS	Distribution Standard System
FRD	Functional Requirements Document

HSI	Human Systems Integration
IT	Information Technology
MAPAF	Military Assistance Program Address File
NSS	National Supply System
OMB	Office of Management Budget
SAMMS	Standard Automated Material Management System
SQL	Standard Query Language
TAC	Transportation Account Code
www	World Wide Web
XML	Extensible Markup Language

## **APPENDIX D - AIR FORCE GEOGRAPHIC ZONE CODES**

<b><u>CODE</u></b>	<b><u>GEOGRAPHIC ZONE</u></b>
1	Nevada, Oregon
2	Arizona, California
3	Colorado, Idaho, Montana, North Dakota, South Dakota, Utah, Washington, Wyoming
4	New Mexico, Texas
5	Arkansas, Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, Oklahoma, Wisconsin
6	Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont
7	Indiana, Kentucky, Michigan, Ohio, West Virginia
8	Alabama, Louisiana, Mississippi, Tennessee
9	Florida, Georgia, North Carolina, South Carolina, Virginia
A	Hawaii, Japan, Philippines, and other Pacific islands
C	Western Canada and Alaska



D	Eastern Canada, Greenland, Labrador, Newfoundland
E	Iceland
F	Netherlands, Europe
H	Panama, Mexico, South America, North Africa, the Caribbean
Blank	Used for CONTROLLED DODAACs