# C2. CHAPTER 2

# DoD ACTIVITY ADDRESS DIRECTORY

C2.1. GENERAL

C2.1.1. Purpose. This chapter implements DoD policy by establishing procedures for the roles, authorities, business rules, governance, and management process of the DoD Activity Address Directory (DoDAAD). The DoDAAD is an interactive, relational database serving as a single authoritative source of identification, routing, and address information for authorized users, including Military Components and Agencies, participating Federal Agencies, authorized contractors, and authorized special program activities such as state and local governments. DoDAAD supports business application systems data and interoperability requirements, including (but not limited to) supply chain, materiel management, distribution, transportation, maintenance, finance, contracting, procurement, and acquisition systems. DoDAAD information is used throughout the federal supply system for identification, requisitioning, shipping, billing, and other uses.

C2.1.2. DoDAAD Composition. The DoDAAD is comprised of both Department of Defense Activity Address Code (DoDAAC) and Routing Identifier Code (RIC) identifiers.

C2.1.2.1. DoDAAC. The DoDAAC is a six-character, alpha-numeric code that uniquely identifies a unit, activity, or organization within the DoDAAD. A unit, activity, or organization may have more than one DoDAAC for different authority codes or purposes. Each activity that requisitions, contracts for, receives, has custody of, issues, or ships DoD assets, or funds/pays bills for materials and/or services is identified by a six-position alphanumeric DoDAAC.

C2.1.2.2. RIC. The RIC is a 3-character, alpha-numeric code that uniquely identifies a unit, activity, or organization that requires system ability to route transactions or receive transactions routed to it (e.g., source of supply) within logistics and financial business systems that use legacy 80 record position format transactions. The RIC was originally conceived to identify an activity in an abbreviated form in the limited MILS data environment, so as not to require the use of the longer six-character activity identifier of a DoDAAC, but its use has since expanded. The first position designates the particular service/agency ownership, the second and third characters are determined by the Central Service Point (CSP). See also paragraph C2.5 of this Chapter.

C2.2. POLICY. The procedures contained in this manual are issued in accordance with the following policy:

C2.2.1. DoDI 4140.01. The “DoD Supply Chain Materiel Management Policy,” December 14, 2011, establishes policy and assigns responsibilities for management of materiel across the DoD supply chain and authorizes the publication of DLM issuances required for the execution of this instruction.

C2.2.2. DoDM 4140.01. The “DoD Supply Chain Materiel Management Procedures,” February 10, 2014, provides policy to establish the DoDAAD Process Review Committee (PRC), which provides the framework for DoDAAC/RIC management and assignment.

C2.3. ROLES AND AUTHORITIES

C2.3.1. Office of the Deputy Assistant Secretary of Defense Supply Chain Integration (ODASD/SCI). The ODASD/SCI will:

C2.3.1.1. Serve as the Office of the Secretary of Defense (OSD) sponsor of the DoDAAD program, issuing policy guidance and instructions for development, expansion, improvement, and maintenance of DoDAAD.

C2.3.1.2. Champion efforts to identify funding sources to support and further the DoDAAD program objectives.

C2.3.1.3. Resolve policy and procedural issues where agreement cannot be achieved within the DoDAAD PRC.

C2.3.1.4. Ensure applicable coordination within OSD staff elements regarding DoDAAD policy guidance or one-time instructional memoranda affecting functions assigned to the DoDAAD PRC.

C2.3.1.5. Support the implementation and use of standard data elements in accordance with policy guidance.

C2.3.1.6. Maintain contact with the PRC through the OSD Principal Staff Assistant (PSA) and the ODASD/SCI PRC member.

C2.3.1.7. Ensure that DoD senior leaders are advised of initiatives and plans as they are developed with respect to DoDAAD.

C2.3.1.8. Monitor PRC activity to ensure compliance with policy, instructions, and standards.

C2.3.1.9. Direct Approved Defense Logistics Management Standards (DLMS) Change implementation dates as needed.

C2.3.2. Defense Enterprise Data Standards Office (DEDSO) DoDAAD System Administrator. As Chair of the DoD DoDAAD Process Review Committee, the DoDAAD Systems Administrator will:

C2.3.2.1. Develop DoDAAD PRC meeting agendas, convene meetings as required, and publish final meeting minutes.

C2.3.2.2. Submit proposed recommendations for DoDAAD improvement to the committee members and the OSD PSA. Present issues to the DoDAAD PRC for review and resolution. Where PRC consensus cannot be achieved, document and present the issues to the OSD PSA for resolution.

C2.3.2.3. Report findings and recommendations of evaluations and reviews, with comments from the DoD Components and participating external organizations, to the OSD PSA through the use of standard DLMS configuration management procedures (e.g., proposed and approved DLMS changes).

C2.3.2.4. Develop business rules and procedure documentation, including business rules for DoDAAD Central Service Point (CSP) and DoDAAD monitor assignment.

C2.3.2.5. Approve and forward CSP and Monitor appointments to the Central Control Point (CCP).

C2.3.2.6. Develop and provide DoDAAD training.

C2.3.2.7. Develop and document DoDAAD functional requirements and specifications.

C2.3.2.8. Ensure testing and validation of approved DoDAAD changes.

C2.3.2.9. Publish the following DoDAAD PRC information:

* current list of DoDAAD PRC members,
* meeting minutes,
* current list of DoDAAD Central Service Points and Monitors,
* DoDAAD System Standard Operating Procedures,
* DoDAAD Master File Layout,
* DoDAAD Assignment Logic information,
* CSP and Monitor appointment memorandum templates, and
* additional DoDAAD resources on the DoDAAD PRC webpage of the DLMS Website.

C2.3.3. DoDAAD PRC. The DoDAAD PRC is a committee responsible for development, maintenance, and change management of the DoDAAD. The committee is chaired by the DoDAAD System Administrator with representation from each of the Services and Agencies who comprise the member subscribers of the DoDAAD. Change management is accomplished through the Proposed DLMS Change (PDC)/Approved DLMS Change (ADC) process. The DLMS change management requirements and guidelines are documented in DLM 4000.25, Volume 1, Chapter 3 (Change Management) and are available on the DLMS Publications page. The DLMS change management process ensures proper documentation of all proposed or approved changes and provides an audit trail for tracking and reporting of these changes to the functional baseline. The DoDAAD PRC operates under the authority and within the framework documented in this chapter. Current PRC members are identified on the DoDAAD PRC webpage.

C2.3.4. DAAS. In addition to being the technical manager of, and organization responsible for the Defense Automated Addressing System (DAAS), DAAS serves as the CCP for the DoDAAD. In this capacity, DAAS is responsible for the following:

C2.3.4.1. Designate a DoDAAD CCP in writing to the DoDAAD System Administrator.

C2.3.4.2. Maintain the DoDAAD as the authoritative data source for DoDAACs and RICs, and the associated data elements.

C2.3.4.3. Maintain a hardware, software, and customer assistance support helpdesk. If users have DoDAAD software related problems, they can call the DAAS customer assistance support helpdesk at 937-656-3247.

C2.3.4.4. Maintain proper system access controls. Access for CSPs and Monitors must be based on both DAAS approved system access requests (SAR), and CSP assignments and Monitor delegations received from the DoDAAD System Administrator.

C2.3.4.5. Maintain system documentation, data validation edits, and security for the DoDAAD.

C2.3.4.6. Maintain a profile of authorized DoDAAD users by access level.

C2.3.4.7. Maintain statistics on the number of accesses and types of access (update, query, download) by user.

C2.3.4.8. Associate DoDAACs and RICs to a unique seven-character CommRI for routing logistics transactions.

C2.3.4.9. Maintain Web query applications.

C2.3.4.10. Maintain the DoDAAD Update Application.

C2.3.4.11. Provide DoDAAD data output to external applications and customers.

C2.3.4.12. Design and maintain the DoDAAD database to implement functional requirements.

C2.3.4.13. Test program functionality and system interface connectivity.

C2.3.4.14. Participate in the DoDAAD PRC.

C2.3.4.15. Review and provide technical input to Defense Enterprise Data Standards Office on DoDAAD PDCs and ADCs.

C2.3.4.16. Implement DoDAAD changes directed in ADCs.

C2.3.5. DoD Components and Federal Agencies. DoD Components and Federal Agencies will:

C2.3.5.1. Appoint a representative, in writing, to the DoDAAD PRC. This representative may be the CSP. A sample appointment letter can be found on the DoDAAD PRC webpage.

C2.3.5.2. Designate, in writing, a primary DoDAAD CSP and an alternate CSP (along with optional DoDAAC monitors) to the DoDAAD System Administrator. A sample letter for these appointments can be found on the DoDAAD PRC webpage.

C2.3.5.3. Submit DoDAAD CSP and Monitor appointment changes to the DoDAAD System Administrator in a timely manner to allow DAAS to promptly add or remove account access to DoDAAD Update Application. Appointments will include all individuals who require access (to include existing appointments) as well as individuals who will be revoked. This will ensure that the latest appointment includes all currently authorized personnel for the Service/Agency. These appointments do not grant access; they authorize access. DAAS grants access based on matching the completed SAR with appointment authorizations.

C2.3.5.4. Develop and publish supplemental procedures for internal use as needed, as long as they do not conflict with the procedures contained herein. Component unique processing information is included in the DoDAAD and is published on the DoDAAD PRC webpage; however, this information remains the Component’s responsibility.

C2.3.5.5. Implement approved DLMS changes.

C2.3.6. DoDAAD Central Service Points. DoDAAD CSPs, designated in writing by their respective Component or Agency, are responsible for the following:

C2.3.6.1. Serve as DoDAAD PRC members or interested parties for their respective Component or Agency.

C2.3.6.2. Assign and maintain DoDAACs and RICs that are authorized in their appointment memoranda for activities of their Service/Agency only.

C2.3.6.3. Advise DAAS of any new COMMRI requirements for DoDAACs or RICs.

C2.3.6.4. Ensure the timeliness, accuracy, and authority for use (authority code) of DoDAAC and RIC information.

C2.3.6.5. Give priority to deploying and redeploying units to ensure that they have current DoDAAC/RIC information prior to their deployment or redeployment.

C2.3.6.6. Monitor and delete contractor DoDAACs upon expiration of the applicable contract.

C2.3.6.7. Promote and support DoDAAD within the respective Component/Agency and serve as the Component’s DoDAAD subject matter expert.

C2.3.6.8. At their discretion, delegate/sub-divide their responsibility for file maintenance of the DoDAACs and RICs for which they are responsible to DoDAAD Monitors, as necessary. Such delegation will be in writing to the DoDAAD System Administrator (see C2.3.5.1. and C2.3.7).

C2.3.7. DoDAAD Monitors. When situations arise whereby services/agencies desire that DoDAAD management be delegated below the CSP level, DoDAAD Monitors can be delegated by the CSP to allow for lower-level management within the service/agency. DoDAAD Monitors are responsible for maintaining DoDAACs/RICs delegated to them by their CSP. DoDAAD Monitors will be appointed in writing by the CSP to the DoDAAD System Administrator and DAAS, identifying the individuals to whom sub-delegations are being made and the DoDAACs/RICs that each is responsible for to allow DAAS to update/remove access to the DoDAAD Update Application as appropriate. See also Special Program DoDAACs below. Monitor appointments will be included in the CSP appointment letter. The CSP and Monitor appointment template can be found at the DoDAAD PRC webpage.

C2.4. DoDAAC AND RIC STRUCTURE. The current list of data elements, descriptions, and business rules that comprise the DoDAAD is found on the DoDAAD PRC webpage. Some of the more common elements of DoDAAC structure are provided below.

C2.4.1. Service and Agency Codes. DoDAACs and RICs are assigned to activities beyond DoD. DoDAAC and RIC assignment is based on MILSTRIP Service and Agency codes identified in DLM 4000.25, Volume 2, Appendix 7.2, Service and Agency Codes. Further stratification of Service and Agency codes for use in creating DoDAACs and RICs are found in the DoDAAD Series Table published on the DoDAAD PRC webpage.

The following are the differing types of DoDAACs that exist:

C2.4.1.1. Department of Defense DoDAACs. DoD Activities are designated by an alpha character in the first position, excluding B, D, G, I, K, O, P, T, X, and Y.

C2.4.1.2. DoD Contractor DoDAACs. DoD contractors (CTR) will only be assigned DoDAACs if they have a contract with DoD that authorizes access to DoD supply system materiel or to provide services such as maintenance/repair that require a shipping address. Contractor DoDAACs may be requested by anyone related to the contract/program through the Contractor DoDAAC request module in the Procurement Integrated Enterprise Environment (PIEE). The requestor will indicate whether the DoDAAC should have requisitioning authority or just be a shipping location. Requisitioning DoDAAC requests will be validated against the contract to confirm the contract allows such authority. In addition to appropriate address information, requestors will ensure the following contract information data elements are entered for every contractor DoDAAC. All are mandatory fields except for Order Number and Contract Period of Performance End date, which are situationally dependent (for all non-contractor DoDAACs, these fields are disabled):

C2.4.1.2.1. Contract Number. The Contract Number is the Procurement Instrument Identifier (PIID) that uniquely represents a contract action or order and its related procurement instrument. It is a 13-character number for DoD contracts, and a 17 character number for Federal Civilian Agency contracts. A contract is a mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing (see FAR Part 2 and Part 4.16). This field is validated against Electronic Document Application (EDA) as a legitimate contract number in PIEE prior to sending to DoDAAD. Like all Contract Information fields, it is not validated in DoDAAD. The DoDAAC of the PIID should cross reference to a DoDAAC that has procurement authority (i.e., the Procurement Authority indicator is checked “Yes” in the DoDAAD). Enter the procurement instrument identifier (PIID). The DoDAAC of the PIID should cross reference to a DoDAAC that has procurement authority (i.e., the Procurement Authority indicator is “Yes” in the DoDAAD).

C2.4.1.2.2. Commercial and Government Entity (CAGE) Code. The CAGE Code must be that of the prime contractor for whom the DoDAAC is being created. Subcontractor CAGEs must never be used.

C2.4.1.2.3. Commercial and Government Entity (CAGE) Name. The name of the owner of the CAGE Code cited shall also be displayed as a contract information data element.

C2.4.1.2.4. Order Number. An Order is a contracting action that is a request for goods or services against an established contract that allows multiple orders, such as an Indefinite Delivery/Indefinite Quantity contract. The order number uniquely identifies the order and its related document. Current policy requires the order number to match the Procurement Instrument Identifier (PIID) format established in FAR 4.16.; however, legacy order numbers may be in varying formats. It is an optional field with a maximum field length of 50 characters.

C2.4.1.2.5. Issuing Office DoDAAC. The Issuing Office DoDAAC is the contracting office that issued the contract under which this contractor DoDAAC is being assigned (see FAR Part 2 for the definition of contracting office). It will be represented by a DoDAAC, which will typically be the same as the first 6 characters of the contract number represented in the Contract Number field (per FAR 4.1603). An Issuing Office DoDAAC must have the Procurement Authority Flag set to “Yes.”

C2.4.1.2.6. Contract Period of Performance End Date. FAR Part 11.4 establishes the requirement to provide a schedule for the delivery or performance of a contract. This field captures the calendar date upon which the delivery or performance period ends in the contract under which this contractor DoDAAC is being assigned. Upon this date, the Authority Code of the CTR DoDAAC is automatically changed to Authority Code 05.

C2.4.1.2.7. Contract Closeout Date. FAR 4.804 establishes the requirement to close out a contract file upon completion of all contract activity. Contracting officers are responsible for closing out related DoDAACs when the contract is closed out (see FAR 51.102). Therefore, when the contract under which this contractor DoDAAC is being assigned has been closed, this DoDAAC will also be closed. If this is a requisitioning DoDAAC, enter the contract closeout date of the contract under which the contractor is performing requisitioning, or if this is a Ship-To DoDAAC, enter the LAST contract closeout date of any contract under which this contractor is performing with this DoDAAC. If closeout date is not known, leave blank. This date sets the Delete Date for the CTR DoDAAC.

C2.4.1.3. Federal Agency DoDAACs. Federal Agency DoDAACs are identified by a G in the first position or by numeric characters in the first and second positions. These may be referred to as Civil Agency Activity Address Codes (AAC). Federal Agency CTR AACs are subject to different rules than those above for DoD CTR DoDAACs.

C2.4.1.4. Special Program DoDAACs. Special Program DoDAACs are identified by a numeric character in the first position followed by an alpha character in the second position. These identify entities that are not limited to a single organizational type and are associated with a special program. Among other purposes, special programs include programs authorized by Congress for state and local entities to purchase materiel from Federal sources. DoD and Federal Agency sponsors of these programs are designated as DoDAAC monitors. Contact the DoDAAD System Administrator for guidance on establishing a DoDAAC series for a special program.

C2.4.2. Addresses. There may be up to four distinct “Type of Address Code” (TAC) addresses for each DoDAAC. CSPs/Monitors will enter the proper address based on the applicable TAC on a letter, label, or box marking in accordance with the applicable mode of transportation. Ensure that only one type of address is used for each of the four address types. Combining part of an Air/Army Post Office (APO) address with a commercial postal standard will create an invalid address. TAC definitions are:

C2.4.2.1. TAC 1 - Owner. TAC 1 identifies the mailing address and other information of the owner and is mandatory.

C2.4.2.2. TAC 2 - Ship-To or Freight. TAC 2 identifies the ship-to or freight address and other information for the activity. If a ship-to address is required (Authority Codes 00, 01, 04, 05 or 06), the TAC 2 must be provided.[[1]](#footnote-2) Addresses listed for freight purposes must contain sufficient information to use the in-the-clear portion of package markings and to insert addresses in the consignee block of transportation documents. The geographic location in the destination block of transportation documents may vary depending upon the mode of transportation. There are two geographic location indicators in addition to the address: Aerial Port of Debarkation (APOD); and Water Port of Debarkation (WPOD). The APOD and WPOD are adjuncts to the address information, and a variance in the address may be required depending on the values in these fields. Supplemental information concerning railheads, airports, etc., serving a given installation in the Continental United States (CONUS) is contained in the Defense Transportation Regulation (DTR). See Table C2.T1.

C2.4.2.3. TAC 3 - Bill-To. TAC 3 identifies the billing address of the activity responsible for bill payments and other information for the activity. If a bill-to address is required (Authority Codes 00, 02, 03, and 04), the TAC 3 must be provided.[[2]](#footnote-3) See Table C2.T1.

Table C2.T1. Authority Code and TAC Rules

| IF | THEN Enter[[3]](#footnote-4) | | |
| --- | --- | --- | --- |
| Authority Code is | TAC 1 | TAC 2 | TAC 3 |
| 00  (Requisition) | YES | YES | YES |
| 01  (Ship-to) | YES | YES | NO |
| 02  (Bill-to) | YES | NO | YES |
| 03  (Do Not Ship-to) | YES | NO | YES |
| 04  (Disposition Services) | YES | YES | YES |
| 05  (Non-Requisition) | YES | YES | NO |
| 06  (Free Issue) | YES | YES | NO |
| 07  (Administrative) | YES | NO | NO |

C2.4.3. Effective and Delete Dates

C2.4.3.1. Effective Date. Effective Date is the date that a change becomes effective. It may be used to schedule future changes. When a DoDAAC is entered or updated and an Effective Date is supplied for a given TAC, the data entered for that TAC will not be effective or published until the current date matches the Effective Date entered. Multiple changes can be entered using this technique, as long as the Effective Date entered does not duplicate an existing Effective Date.

C2.4.3.2. Pending Effective Date. When an Effective Date is pending for a given TAC, Defense Automatic Addressing System Inquiry (DAASINQ)/Enhanced Defense Automatic Addressing System (eDAASINQ) will indicate the pending date by flagging the TAC with a graphic above the Effective Date field indicating “Future DoDAAD information available”. To view the pending changes, the user may click the “Future data available” graphic.

C2.4.3.3. Deletion Date. The Deletion Date is used to delete a DoDAAC. Any DoDAAC with a Deletion Date that has passed is considered a deleted DoDAAC. A deleted DoDAAC will remain inactive on the DoDAAD master file for six years and three months before the record is permanently purged from the master file. During this period, a deleted DoDAAC prevents requisition transactions from being processed through DAAS; however, outstanding interfund bills (with the bill-to authorized in accordance with the DoDAAC authority code) that are associated with previously processed requisitions will not reject due to an invalid DoDAAC during this period. After the six years and three months period, once the deleted DoDAAC is physically removed from the DoDAAD, all subsequent requisitions or bills would reject due to an invalid DoDAAC. This is only true, however, for transactions processing through DAAS. For any transactions that process either through the Global Exchange (GEX) or some other means other than DAAS, a deleted DoDAAC will prevent those transactions from processing even during that period of being deemed inactive. The only indication that a DoDAAC has been deleted during that time is the existence of the Deletion Date on the master record for the given DoDAAC. No new requisitions may be initiated for a deleted/inactive DoDAAC. CSPs or monitors may restore a deleted DoDAAC, but they may not reassign it to another address during the six years and three months retention period.

C2.4.3.4. Pending Deletion Date. When a Deletion Date is pending for a DoDAAC, DAASINQ/eDAASINQ will indicate the pending date by flagging the DoDAAC with a graphic above the Deletion Date field indicating “Future data available.” To view the pending changes, the user may click the “Future data available” graphic.

C2.4.4. Additional Codes. In addition to addressing information and effective and delete dates, the following codes are DoDAAD data elements critical to enabling business processes across the DoD:

C2.4.4.1. Organization Type Code. The Organization Type Code is a one-character code used to identify the type of organization for which the DoDAAC associates, categorically. Those categories include:

* D = DoD and USCG
* F = Federal Agencies – Non-DoD and USCG
* S = State/Local
* N = NGO
* X = Foreign

C2.4.4.2. Authority Codes. CSPs (or DoDAAC monitors as applicable) must assign an authority code for each DoDAAC. The authority code restricts the use of the DoDAAC. DoDAAC authority codes are applicable to all Components/Agencies, and there are many supply and finance business process edits based on the authority code. Authority Code 00 allows unrestricted use of the DoDAAC. The remaining codes limit the use of the DoDAAC for unique and specific purposes, such as bill-to only or ship-to only. Table C2.T2 identifies the current DoDAAC Authority Codes.

| Table C2.T2. DoDAAC Authority Codes | | |
| --- | --- | --- |
| Code | Description | Definition |
| 00 | Requisition | Authorized to initiate a requisition/purchase for goods and services. Authorized ship-to and bill-to. |
| Required[[4]](#footnote-5): TAC[[5]](#footnote-6) 1, TAC 2, TAC 3 | |
| Restriction: None | |
| Business Rules: Can be used for any business process. | |
| DAAS DoDAAC Authority Code Edit: No additional edit. | |
| 01 | Ship-To Only | Can only be used as a ship-to address with no other implicit authority. |
| Required: TAC 1, TAC 2 | |
| Restriction: Not authorized for requisition or bill-to. | |
| Business Rules: Used as a ship-to designation. | |
| DAAS DoDAAC Authority Code Edit: DoDAAC may only be used in the MILSTRIP legacy requisition supplementary address field (record positions 45-50) with signal code J, L, M, X. Under DLMS, DoDAAC may not be used in N101 with codes OB, BT, and BS, and may not be used in N901 with code TN. | |
| 02 | Finance (Bill-to Only) | DoDAAC can only be used as a bill-to. |
| Required: TAC 1, TAC 3 | |
| Restriction: Cannot requisition or be used as a ship-to designation. | |
| Business Rules: Used as a bill-to designation. | |
| DAAS DoDAAC Authority Code Edit: DoDAAC may only be used in the MILSTRIP legacy requisition supplementary address field (record positions 45-50) with signal code B. Under DLMS, DoDAAC may not be used in N101 with codes OB, ST, Z7 and BS, and may not be used in N901 with code TN. | |
| 03 | Do Not Ship-to | Cannot be used as a ship-to designation. |
| Required: TAC 1, TAC 3 | |
| Restriction: Cannot be used as a ship-to designation. | |
| Business Rules: Can requisition or be used as a bill-to designation. | |
| DAAS DoDAAC Authority Code Edit: If DoDAAC used in the MILSTRIP legacy requisitioner field (record positions 30-35), it must contain signal code J, K, L, M, or X. If used in the requisition supplementary address field (record positions 45-50, it must contain signal code A, B, C, or D. Under DLMS, DoDAAC may not be used in N101 with codes ST, Z7 or BS. | |
| 04 | DLA Disposition Services Only | DLA Disposition Services Only (e.g., State agencies surplus). Used to identify activities that have no requisition authority other than for DLA Disposition Services Only materiel. |
| Required: TAC 1, TAC 2, TAC 3 | |
| Restriction: Cannot requisition new materiel. Only authorized to obtain materials from DLA Disposition Services (DOD excess only). | |
| Business Rules: Although the material is normally provided as a free issue; in some instances a cost may be required. Consequently, TACs 1 through 3 are required to cover every possibility. | |
| DAAS DoDAAC Authority Code Edit: DoDAAC may only be used with DLA Disposition Services RIC (S9D) in record positions 4-6. Under DLMS, DoDAAC may only be used with DLA Disposition Services RIC (S9D) in RIC To. | |
| 05 | Non-Requisition | Cannot initiate a purchase or request for goods and services. |
| Required: TAC 1, TAC 2 | |
| Restriction: Cannot requisition/purchase goods/services. | |
| Business Rules: Used as a ship-to designation. | |
| DAAS DoDAAC Authority Code Edit: DoDAAC cannot be used in the MILSTRIP legacy requisitioner field (record positions 30-35). Under DLMS, DoDAAC cannot be used as N101 code OB or N901 code TN. | |
| 06 | Free Issue | No cost option. The activity is restricted to items that are available without cost (e.g., DLA Disposition Services, NGA Maps). |
| Required: TAC 1, TAC 2 | |
| Restriction: Cannot requisition/purchase any good/services. | |
| Business Rules: Similar to DLA Disposition Services, but can request free of cost items (e.g., maps from National Geospatial-Intelligence Agency (NGA)). Can be used as a ship-to designation. | |
| DAAS DoDAAC Authority Code Edit: DoDAAC may only be used with signal code D or M. Under DLMS, DoDAAC may only be used with PO105 code NC. | |
| 07 | Administrative | Administrative only. This code is used for information/identification purposes only (e.g., Defense Courier Service (DCS), or contingency/emergency use). |
| Required: TAC 1 | |
| Restriction: Cannot requisition, be used as a ship-to- designation, or be used as a billing designation (TAC 2 and TAC 3 are not allowed). | |
| Business Rules: Information/identification use only. | |
| DAAS DoDAAC Authority Code Edit: DoDAAC may not be used in MILSTRIP legacy requisition in record positions 30-35 or in record positions 45-50 as a “ship to” or “bill to”. Under DLMS, DoDAAC cannot be used with N101 codes OB, BT, BS, ST, or Z7 or in N901 code TN. | |

C2.4.4.3. Major Command Codes (MAJCOM). MAJCOMs allow sub-delegation of DoDAACs below the service/agency level. These codes are service/agency-created and are denoted in the DoDAAD by the header “MAJ\_COMMAND.” The current MAJCOMs are maintained by DAAS and are published on the DoDAAD PRC webpage.

C2.4.4.4. Contractor Flag. The Contractor indicator or “flag” is a VARCHAR with a value of either “Y” for yes or null for no, that designates whether or not the DoDAAC is for a contractor. For DoD contractor DoDAACs, this flag is automatically set based on the DoDAAC Series (i.e., approved contractor DoDAAC Series will automatically set the flag to “Y”). For the Federal Agencies, this flag, when marked with a “Y” will designate it as a contractor and will require the mandatory Contract Information fields to be completed. The Contractor Flag can only be set when the Org Type Code is “F” or “D.”

C2.4.4.5. Common Governmentwide Accounting Classification (CGAC) Code. The CGAC is a three-digit code used by the Federal Government to identify an Agency (Department) of the Federal Government at the highest tier (i.e., Department of Agriculture is 012). CSPs will set this code for only Government DoDAACs and will set it based on which tier the DoDAAC belongs. For instance, if DLA creates a DoDAAC for the U.S. Army, the CGAC of the DLA-created DoDAAC would cite U.S. Army (020) and not DLA, because the DoDAAC is for a U.S. Army activity. The CGAC does not apply to contractors, state/local activities, foreign entities, and non-government organizations (NGOs).

C2.4.4.6. Sub Tier Code. The Sub Tier Code is a four-digit code that identifies an organizational level of an Agency below the highest tier. The first two characters are the two-digit Treasury Agency Code (the same as the first two positions of a Federal Agency DoDAAC), and the third and fourth characters are the Sub Tier of the Agency, more commonly referred to as a bureau. The Agency Code, therefore, identifies the ‘sub tier’ to its respective Agency, in one, four-digit code. This code has no relationship to either the Major Command Code (MAJ\_COMAND) or the GSA Bureau Code (GSA\_BUREAU\_CD) and is used in the Federal Procurement Data System to identify entities below the Agency level. CSPs will set this code for any record that identifies an activity performing actions that include contract writing, funding, and/or awarding of grants. It does not apply to non-Government activities. As such, it is a mandatory field when the Procurement Authority flag is set, and only when the Org Type Code is “F” or “D.” For DoD Components, the Sub Tier Code is based on the Treasury Agency code and “00” (i.e., Navy = 1700).

C2.4.4.7. DoDAAC Purpose Codes. The DoDAAD has several purpose code flags that identify how a DoDAAC is used by a particular business domain (e.g., procurement, grants). The following are the Purpose Code flags that exist in the DoDAAD:

C2.4.4.7.1. Procurement Authority. Procurement Authority is a legal authority, delegated down from the Department level to entities of the Federal Government who are authorized to award contracts which obligate the Government to binding agreements with commercial and other government entities. For the DoD, this authority is delegated by the Secretary of Defense through the Undersecretary of Defense for Acquisition, Technology and Logistics (AT&L), Defense Procurement and Acquisition Policy (DPAP) and by the Senior Accountable Officials (SAO) of the Federal Agencies. The Procurement Authority flag will be set to “Y” to identify activities that have been delegated this authority and that are legally authorized to award contracts. The Procurement Authority Flag can be marked in association with any other existing Purpose Code. When this flag is set, it will make the Sub Tier Code and CGAC mandatory field entries. This flag can only be set if the Org Type code is “F” or “D.”

C2.4.4.7.2. Grant Authority. Grant Authority identifies an activity/office that has been delegated, by the head of a DoD or Federal Civilian Agency, the legal authority to make and manage awards under the auspices of a designated grants officer. In DoD, the office’s DoDAAC must be used to construct the grants award identifier. Civilian agencies may use the AAC in their award identifiers. The Grant Authority flag will be set to “Y” to identify an activity/office that has the authority to award grants, cooperative agreements, or federal financial assistance vehicles. The Grant Authority Flag can be marked in association with any other existing Purpose Code. When this flag is set, it will make the Sub Tier Code and CGAC mandatory field entries. This flag can only be set if the Org Type code is “F” or “D.”

C2.4.4.7.3. Funding Office. The Funding Office flag represents that the office identified by the DoDAAC/AAC has the ability to initiate requirements (e.g., the office has a budget and can initiate requirements packages that will result in contracts, grants, and other types of awards). This flag is not to be used to represent financial entitlement or disbursing functions. The Funding Office Flag can be marked in association with any other existing Purpose Code (i.e., it is not mutually exclusive with Procurement or Grants). When this flag is set, it will make the Sub Tier Code and CGAC mandatory field entries. This flag can only be set if the Org Type code is “F” or “D.”

C2.4.4.7.4. Contract Administration Office (CAO). The CAO flag indicates that the office identified by the DoDAAC has the authority and capability to perform contract post-award (FAR 42.3) functions. The CSP should only make this change based on input from PIEE. The CAO flag can be marked in association with any other existing Purpose Code (i.e., it is not mutually exclusive with Procurement or Grants). When this flag is set, it will make the Sub Tier Code and CGAC mandatory field entries. This flag can only be set if the Org Type code is “F” or “D.”

C2.4.4.8. Standard Point Location Code (SPLC). The Military Surface Deployment and Distribution Command (SDDC) is required to maintain accurate and current Standard Point Location Code (SPLC) values in its DoDAAC-to-SPLC cross-reference File. The National Motor Freight Traffic Association (NMFTA) creates, maintains, and publishes via a subscription all valid SPLC assignments. DAAS maintains and administers the SPLC maintenance in the Department of Defense Activity Address Directory (DoDAAD) in support of the Defense Transportation Payment Program. DAAS ensures that accurate, timely data and coding is in place to support all critical elements in support of the Defense Transportation Payment Program.

C2.4.4.9. Accounting Disbursing Station Number/Fiscal Station Number (ADSN/FSN). This code identifies the Service payment office. This field is not validated within the DoDAAD; rather, it is Service defined and Service dependent. The Army and Air Force set a five-digit numeric code, while the Navy and Marine Corps mostly use a DoDAAC. DLA and Other DoD Activities (e.g., WHS, NSA, etc.) use a mix of numeric codes and DoDAACs.

C2.4.4.10. Consolidation and Containerization Point (CCP). The code applies when supplies are to be consolidated for onward movement by SEAVAN or 463L pallets. The codes are defined in the USTRANSCOM Reference Data Management (TRDM) and then select DTR Data and Consolidation Containerization Point.

C2.4.4.11. Break Bulk Point (BBP) or RIC\_DODAAC. The BBP DoDAAC denotes the location to which multi-consignee shipments (e.g., SEAVANS) are shipped and broken into smaller shipment for onward movement to the ultimate consignee. NOTE: the same file layout is used by both the DoDAAD and RIC. If the record is a RIC, the BBP is referred to as the “RIC DoDAAC” and holds the DoDAAC associated to the RIC.

C2.4.4.12. Aerial Port of Debarkation (APOD). The APOD is defined as the final destination aerial port for OCONUS shipments. The APOD codes are in the TRDM, and then select DTR Data and Aerial Ports. DAAS downloads a table of APOD information from USTRANSCOM to load the drop-down values in the DoDAAD update application. A new copy of the APOD is downloaded every time the table is updated by USTRANSCOM. APOD is required if outside the CONUS.

C2.4.4.13. Water Port of Debarkation (WPOD). The WPOD is defined as the final destination Surface Port for OCONUS shipments. The WPOD (also known as SPOD) codes are in the TRDM and then select DTR Data and Water Port. DAAS downloads a table of WPOD information from USTRANSCOM to load the drop-down values in the DoDAAD update application. A new copy of the WPOD is downloaded every time the table is updated by USTRANSCOM. WPOD is required if outside the CONUS.

C2.4.5. DoDAAC Assignment Logic. In some instances, components have assigned DoDAACs in a logical sequence within their assigned series. Service/Agency DoDAAC Assignment Logic is published on the DoDAAD PRC webpage.

C2.4.6. Unique Processing Rules. Some Services and Agencies have additional unique processing rules that are applicable solely to their respective Service/Agency. Current Service/Agency specific unique processing rules are published on the DoDAAD PRC webpage

C2.5. ROUTING IDENTIFIER CODES

C2.5.1. Purpose. The use of the RIC has evolved over time. Its original intended purpose was to identify an activity with only three characters, for the routing of MILS transactions to and/or from that activity. Every RIC must associate to one DoDAAC (the RIC\_DODAAC), and any activity (DoDAAC) that requires MILS routing can only have one RIC to identify it. The RIC’s Type Address Code (TAC) must match the TAC 1 of the associated RIC\_DODAAC.

C2.5.2. The TAC address was intended to be used for the mailing of paper documents to the activity for processes that were not automated by MILS transactions (e.g., proofs of delivery, reports of discrepancy, material inspection and receiving reports (DD250), etc.). The mailing of such documents has been largely replaced by DLMS transaction exchanges. Since this is a mailing address, RICs are not used for shipping. The RIC associates to a DoDAAC. if a shipping action is required to that activity, shippers must use the TAC2 of the associated DODAAC as the freight address for cargo movements.

C2.5.3. The DoDAAD is the official repository for DoDAACs and RICs, and DAAS is the agent responsible for maintaining the DoDAAD, as well as for enforcing the data validation editing, routing, and electronic transmission of logistics transactions to the DoD Components, Federal Agencies, and contractors.

C2.5.4. CSPs/Monitors establishing or changing DoDAACs or RICs need to verify they set the correct COMMRIs for their DoDAACs/RICs to ensure legacy 80 rp/DLMS logistics transactions (e.g., requisitions and supply/shipment status) are properly routed to their DoDAACs and RICs. Customers that already have DAAS accounts (i.e., DIELOG, WEBREQ, WEBVLIPS, DAMES, DDN, MQ, etc.) must provide the CSPs the preferred account COMMRI to direct their logistics transactions status.

C2.5.5. To qualify for assignment of a RIC, the activity must have an assigned DoDAAC and be an integral and predetermined element of an established legacy logistics system and which activity requires the ability to route legacy (80 rp) transactions.

C2.5.6. RICs are maintained within the DoDAAD by CSPs and Monitors who serve as the focal point for receipt of all RIC additions, changes, and/or deletions. DAAS will monitor RIC code assignment for compliance with the above assignment rules. Interested parties may interrogate the DoDAAD for RICs through the eDAASINQ on the DAAS Website (CAC Required).

C2.6. DoDAAD UPDATES. There are three methods for CSPs or their designated DoDAAD Monitors to update the DoDAAD. They are contained in the DoDAAD System Standard Operating Procedures (SOP). The DoDAAD System SOP provides detailed DoDAAD update information and can be found on the DoDAAD PRC Page of the DEDSO Website.

C2.6.1. DoDAAD Update Application

C2.6.1.1. DAAS maintains a DoDAAD Update Application for updating DoDAACs/RICs that is available to all designated DoDAAD CSPs and delegated Monitors for real-time DoDAAD updates. This application incorporates all approved validations and edits. It facilitates real-time validation, elimination of erroneous data, elimination of major reconciliations, and automated file synchronization processing. It also provides easy additions and modifications of DoD Component unique data elements. Access to the DoDAAD Update Application is controlled in accordance with DoD Public Key Infrastructure (PKI)/Common Access Card (CAC) requirements and requires an appointment memorandum submitted to the DoDAAD System Administrator, and a SAR submitted to DAAS.

C2.6.1.2. DAAS deactivates accounts when a DoDAAC CSP/Monitor is no longer authorized or when the account has not experienced activity for a period of time determined by DAAS. CSPs/Monitors are restricted through access controls to DoDAACs and RICs authorized in their appointment letter. CSPs are unable to access other Component/Agency DoDAACs or RICS. For example, an Army CSP is not able to access Navy DoDAACs or RICs.

C2.6.2. Army and Air Force Update Applications. The Army and Air Force CSPs may also use their respective DoDAAD maintenance applications. The Army and Air Force are responsible for ensuring that their respective applications provide the same capabilities and data validation edits as the DoDAAD Update Application. Completed maintenance actions will update the single authoritative source database at DAAS in near real-time.

C2.7. DoDAAD OUTPUT. The following are the authorized means by which to receive DoDAAD data output:

C2.7.1. Web Services. Web Services provides Component application systems near, real-time access to the DoDAAD database and is the preferred method for applications to access DoDAAD data. Contact the DAAS Help Desk concerning DoD Data Services (DDATA) Web Services at daashelp@dla.mil.

C2.7.2. Database Replication. Database replication provides near, real-time access to a copy of the authoritative source. DAAS uses a replication process to synchronize local copies of the DoDAAD database with the authoritative database on a scheduled basis. Scheduled updates are determined by the system requesting the replication and can be on any timeframe up to every 15 minutes. No new data replication processes will be authorized; however, current replication accounts will be migrated to Web Services based upon DLA directives and customer capabilities. Please contact the DAAS Help Desk concerning DDATA Database Replication/Web Services.

C2.7.3. Secure File Transfer Protocol. DAAS issues secure file transfer protocol (SFTP) accounts for the purpose of retrieving customer required DoDAAD-related data created by applications that have direct access to various DAAS data repositories. These individual user accounts are monitored to access daily, weekly, and monthly data. There is a data refresh lag time due to the batch processing for file creation and staging for customer pickup. The batch file formats are one form of SFTP output (see C2.6.3). This is the least preferred data access method for obtaining DoDAAC data. The procedures to access and use SFTP accounts are available on the DAAS Website.

C2.7.4. DAASINQ. Users can query and view DoDAACs and RICs via the web-based DAASINQ application at any time. DAASINQ is open to all users. It requires the user to know and enter the DoDAAC or RIC desired, and it returns information for only that single DoDAAC or RIC. The procedures for accessing and using DAASINQ are available on the DAAS Website.

C2.7.5. eDAASINQ. Users can view, query, and download DoDAAD query results for DoDAACs and RICs via the web-based eDAASINQ application at any time. This is a robust query enabling wild card searches of data with downloading capability. The user must have a CAC or PKI certificate and a SAR submitted to DAAS. Users must consider operational security in protecting and distributing query results. The procedures to access and use eDAASINQ are available on the DAAS Website.

C2.8. DoDAAD DATA SECURITY. The DoDAAD will be marked and handled by all users as Controlled Unclassified Information (CUI).

C2.8.1. The aggregated content of the DoDAAD (i.e., multiple DoDAACs and/or RICs and their respective data elements) is exempted from Public Release under the Freedom of Information Act (5 U.S.C. § 552(b)(3)) because it meets the requirements for exemption under 10 U.S.C. § 130e. Specifically, the DoDAAD database, as a single authoritative source for the Department of Defense (DoD) business enterprise architecture, qualifies as DoD critical infrastructure security information (CISI). CISI is categorized as CUI, and as defined by 10 U.S.C. § 130e, it includes:

“…sensitive but unclassified information that, if disclosed, would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to Department of Defense operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated by or on behalf of the Department of Defense, including vulnerability assessments prepared by or on behalf of the Department of Defense, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security.”

C2.8.2. The DoD Director of Administration and Management (DA&M) has issued a Determination that the DoDAAD meets this definition of CISI, because it is comprised of both DoDAACs and RICs in an interactive relational database serving as a single authoritative source of identification, routing, and address information for authorized users, including Military Components and Agencies, participating Federal Agencies, authorized contractors, and authorized special program activities such as state and local governments.

C2.8.3. DoDAAD supports business application systems data and interoperability requirements, including (but not limited to) supply chain, materiel procurement, and acquisition systems. Each activity that requisitions, contracts for, receives, has custody of, issues, or ships DoD assets, or funds/pays bills for materials and/or services is identified by a DoDAAC (six-position alphanumeric code).

C2.8.4. DoDAACs are used in a myriad of business systems spanning the entirety of the DoD’s business enterprise architecture, including acquisition, procurement, contracting, requisitioning, shipping, billing, pay, maintenance, installations management, human resources, energy resources, and the accountability and requisition of ordnance, ammunition, and perishables in logistics systems across the DoD. DoDAACs are also used for business operations involving the accountability of property and facilities, as well as for hazardous material management. Access to the DoDAAD allows access to these DoDAACs. When coupled with access to other unclassified logistic systems, users are provided with multiple data points which, when combined, disclose location of materials and operational status and plans. The contents of the DoDAAD are sensitive for a number of reasons:

• DoDAACs are created to support sensitive operations and to facilitate the business process associated with them.

• DoDAACs for the following locations include names of employees and Service members as well as duty station addresses for:

1. Department of Defense installations and ports that are outside the contiguous United States (OCONUS).
2. Deployed units and activities performing real world contingency operations or exercises from both contiguous United States (CONUS) and OCONUS bases.
3. Ships afloat.
4. Ships still in CONUS ports but scheduled to go afloat.
5. Ships still in OCONUS ports but scheduled to go afloat.
6. Embassies.
7. War Reserve Equipment sets pre-positioned OCONUS.

C2.8.5. In addition, a DoDAAC could be used in an unauthorized way whereby the internal controls of the Agency can be circumvented and appropriations obligated without the proper authority being involved in the process. A DoDAAC is very much like a credit card number which, in the wrong hands, can be used to spend money without the rightful “owner” of the code (i.e., the entity with authority to use the code) being aware that the Agency’s appropriations are being spent. Individuals have been prosecuted who have used a DoDAAC to purchase items (i.e., televisions) for personal gain. Therefore, effective management, control, and use of DoDAACs by all DoD Components is critical to ensure DoD fiscal responsibility.

C2.8.6. If the DoDAAD were released, it would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities related to critical infrastructure or protected systems owned or operated by or on behalf of the DoD.

C.2.8.7. If an adversary of the United States Government had the DoDAAD, they could determine the issuance of orders; the movement of specially qualified personnel to units and the installation of special capabilities, as well as the conduct of activities in a way that will reveal intensification of preparations before initiating operations. From this information, the adversary could identify very sensitive DoD activities including clandestine locations of DoD activities, force structure, and even troop movement.

1. Refer to ADC 1117. This requirement is not retroactive to DoDAACs established prior to July 2, 2014. [↑](#footnote-ref-2)
2. Ibid. [↑](#footnote-ref-3)
3. YES indicates the TAC is required. NO indicates the TAC is optional. [↑](#footnote-ref-4)
4. Required means minimum required data element(s) [↑](#footnote-ref-5)
5. TAC means Type of Address Code [↑](#footnote-ref-6)