

Navy Rules for Permissions and Accesses to the Defense Travel System

Defense Travel System (DTS) Separation of Duty rules are applicable to Navy and will be followed to comply with the DoD FMR Vol. 5. Ch. 1, 010305.B and Ch.5, 050201.A, DoDI 5154.31 Vol. 3, NAVADMIN 393/11, NAVSUPINST 4650.8, and the Navy DTS Business Rules as it relates to roles, permissions and accesses within DTS. DTS roles that can be held are listed with similar role types in the tables below. Individuals may **only** perform DTS role(s) that are contained in each table at a time with appropriate permission levels and accesses. However, if compliance to these rules cannot be obtained due to manpower, turnover, training, back-ups, unforeseen circumstances and/or temporary organizational events in order to meet mission requirements, etc, a temporary SOD waiver may be requested. Requests for SOD waivers are to be submitted to the Navy DTS Program Management Office via the MAJCOM LDTA using the SOD Waiver Request Form. Justifications and management controls must be stated in detail on the SOD Waiver Form and thoroughly vetted by the MAJCOM LDTA prior to submission to the Navy DTS PMO. **Waivers are temporary in nature until further notice by the Navy DTS PMO.**

DTS ADMINISTRATORS	
Lead Defense Travel Administrator (LDTA)	Should not be in any routing list or create, edit or adjust any traveler's document. The LDTA will be held at the MAJCOM level. Each MAJCOM will only have one LDTA and at least one Alternate LDTA. MAJCOM LDTAS should provide necessary DTS support to all subordinate command level ODTAs.
Organization Defense Travel Administrator (ODTA)	Should not be in any routing list or create, edit or adjust any traveler's document. ODTA's will support the MAJCOM LDTA and provide necessary DTS support to subordinate commands.
Finance Defense Travel Administrator (FDTA)	Should not be in any routing list and will not create, edit or adjust any traveler's document. FDTAs will contact the traveler, NDEA or travel clerk to correct DTS documents that have rejected from their appropriate accounting system/entitlement pay system.
Budget Defense Travel Administrator (BDTA)	Should not be in any routing list or have the ability to create, edit or adjust any traveler's document.
Debt Management Monitor (DMM)	Should not be in any routing list or have the ability to create, edit or adjust any traveler's document.

INVOICE PROCESSING	
Centrally Billed Account Specialists (CBAS)	Should not be in any routing list and may only T-ENTER documents for the purposes of correcting CBA ticketed transactions for reconciliation. <i>(See Note 5 on pg.3)</i>

DOCUMENT ROUTING	
Non-Approving Routing Official (RO)	Can apply any DTS routing stamps other than the APPROVED Stamp. Should never have permission levels 3, 4, 5, or 6, and no group access.
Authorizing/Approving Official (AO)	Can apply the APPROVED stamp in DTS. Should never have permission levels 3, 4, 5, or 6, and no group access.

DOCUMENT PROCESSING	
Non DTS Entry Agent (NDEA)	Should never be in any routing list and should never have Organizational access. <i>(See Note 6 on pg.3)</i>
Travel Clerk/Preparer	Should never be in any routing list and should never have Organizational access. <i>(See Note 6 on pg.3)</i>

SOD MATRIX

Users CANNOT perform more than one "Role Type" listed below in DTS (i.e. if your current DTS role falls under two different colors, that would constitute a SOD violation).

Role Type	Position	Permission Level(s)	Can also be in Routing list	Organization Access	Group Access	Read Only Access Administrator/User	Special Profile Indicator(s)
A D M I N I S T R A T I O N	LDTA	0,1,2,3,4,5,6 <i>*Note 1</i>	No	<ul style="list-style-type: none"> Four Char MAJCOM Org Code, e.g, "DN11" 	<ul style="list-style-type: none"> Four Char MAJCOM Code, e.g, "DN11" 	<ul style="list-style-type: none"> Administrator Four Char MAJCOM Code, e.g. "DN11" <i>*Note 2</i> 	<ul style="list-style-type: none"> Manually Entered Transaction Non-DTS Entry Agent (T-Entered) Debt Management Monitor Self-AO Approval
	ODTA	0,1,2,3,4,5,6* <i>*Note 1</i>	No	<ul style="list-style-type: none"> Top Level Org code of ODTA's AOR <i>*Note 1</i> 	<ul style="list-style-type: none"> Top Level Group code of ODTA's AOR <i>*Note 1</i> 	<ul style="list-style-type: none"> User/Administrator Top Level Org code of ODTA's AOR <i>*Note 4</i> 	<ul style="list-style-type: none"> <i>See Note 1</i>
	FDTA	0, 1, 3, 5, 6 <i>*Note 3</i>	No	<ul style="list-style-type: none"> Top Level Org code of FDTA's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> User Top Level Org code of FDTA's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> Manually Entered Transaction <i>*Note 3</i>
	BDTA	0,1,3 <i>*Note 3</i>	No	<ul style="list-style-type: none"> Top Level Org code of BDTA's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> User Top Level Org code of BDTA's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> Manually Entered Transaction <i>*Note 3</i>
	DMM	0,6 <i>*Note 3</i>	No	<ul style="list-style-type: none"> Top Level Org code of DMM's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> Top Level Group code of DMM's AOR <i>*Note 7</i> 	<ul style="list-style-type: none"> User Top Level Org code of DMM's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> Debt Management Monitor <i>*Note 3</i>
Invoice Processing	CBAS	0, 4 <i>*Note 3</i>	No <i>*Note 5</i>	<ul style="list-style-type: none"> Top Level Org code of CBAS's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> Top Level Group code of CBAS's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> User Top Level Org code of CBAS AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> Non-DTS Entry Agent (T-Entered) <i>*Note 3, 5</i>
Document Routing	RO	0,2 <i>*Note 3</i>	Yes <i>*Note 3</i>	<ul style="list-style-type: none"> Top Level Org code of RO's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> User Top Level Org code of RO's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> None
	AO	0, 1, 2 <i>*Note 3</i>	Yes <i>*Note 3</i>	<ul style="list-style-type: none"> Top Level Org code of AO's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> User Top Level Org code of AOs AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> None
Document Processing	TRAVEL CLERK	0, 5 <i>*Note 3, 6</i>	No	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> Top Level Group code of Travel Clerk's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> None
	NDEA	0, 5 <i>*Note 3. 6</i>	No	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> Top Level Group code of NDEA's AOR <i>*Note 3</i> 	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> Non-DTS Entry Agent (T-Entered) <i>*Note 3</i>

***Note 1** – MAJCOM LDTA's will authorize and grant all Permission Level (s), Organization Access, Group Access, Profile Indicator(s) and Read Only Access (User/Administrator) to their appropriate ODTAs. The MAJCOM LDTA will determine if ODTAs will be granted a PL6. If ODTA's are given PL6 then the MAJCOM LDTA needs to decide if the ODTA will be able to grant others PL6 or if that responsibility will strictly be limited to the MAJCOM LDTA. PL3 grants DTAs the ability to update EFT data in a traveler's profile in the DTA maintenance tool.

***Note 2** – MAJCOM LDTA's will have Read Only **Administrator** access for their command. MAJCOM LDTAs may grant ROA **User** access throughout the command as needed and may **only** grant ROA **Administrator** access to Command ODTAs. All additional ROA Administrator access may be granted by submitting a ROA REQUEST FORM to the Navy DTS PMO.

***Note 3** – ODTA's will authorize and grant all Permission Level (s), Organization Access, Group Access, and Profile Indicator(s) to appropriate DTS positions of appointment. ODTAs may only grant ROA **User** access within AOR if given ROA Administrator access by the MAJCOM LDTA.

***Note 4** – ODTA's may have ROA **User** access or ROA **Administrator** access as determined and granted by their MAJCOM LDTA in their appropriate Area of Responsibility (AOR). ODTAs may only grant ROA **User** access within AOR if given ROA Administrator access by the MAJCOM LDTA.

***Note 5** – CBAS will have the NDEA indicator for the purposes of correcting CBA ticketed transactions for reconciliation and should not be placed on any routing list or special routing list for CBA.

***Note 6** – NDEAs/Travel Clerks will have permission level 5 for the purposes of having the ability to refresh the EFT data link in a traveler's document in the event EFT data is updated in a traveler's profile.

***Note 7** – DMMs will have Group Access in order to view and access all DUE US documents in the DMM Gateway. Without Group Access, the DMM Gateway will not show any DUE US documents for processing.

PERMISSIONS LEVELS AND ACCESSES

Permission Level 0 – Allows a user to create and sign their Authorizations, Local Vouchers and Vouchers and make adjustments and/or amendments to their document

Permission Level 1 – Allows a user access to the Budget Module to “view-only” budget information and budget reports

Permission Level 2 – Allows a user to apply a stamp in the “Route & Review” document process

Permission Level 3 – Allows a user to view, add, edit, and generate Budget reports in the Budget module

Permission Level 4 – Along with account activation, allows a user access to the Centrally Billed Accounts (CBA) module

Permission Level 5 – Along with Permission Levels 0,1,3,6, allows a user access to the DTS Maintenance Tool to add, edit and delete Organizations, routing lists, groups, user/traveler profiles, and LOAs.

Permission Level 6 – Allows a user access to the Debt Management Monitor (DMM) Module and add, edit and delete LOAs, along with Permission Level 5, in the Maintenance Tool.

Organizational Access – Allows a user to run reports in the Report Scheduler at the Organizational level granted; Along with Permission Levels 0,1,3,5,6, allows a user to add, edit, and delete Organizations, routing lists, groups, user/traveler profiles, and LOAs at the Organizational level granted.

Group Access – Allows a user to go into “Traveler Lookup” to access, view and edit documents of travelers belonging to the group assigned.

ROA Access – Allows a user to “view-only” traveler documents under Administration > ROA Trip with designated ROA Organizational access.

ADDITIONAL ROLES, ACCESSES AND RESPONSIBILITIES:

- ❖ **Navy DTS PMO** – Under provisions outlined in the OPNAV INSTRUCTION 4650.15C, the Navy DTS Program Management Office will require all DTS permissions and accesses in order to sufficiently administer, maintain, evaluate, audit and provide quality service to the Navy Defense Travel Program for all TDY travelers under the Department of Navy.
- ❖ **Contractor DTS Support** – As delegated by the Command or specified in a Contractor Support Letter, contractors can perform various roles in DTS. Contractors must adhere to the same rules as stated above in maintaining SOD compliance and may not perform any support roles that fall in different tables as listed above. If compliance cannot be obtained, a temporary SOD waiver can be requested. Below are the DTS roles that can be performed by contractors:
 - **DTS Administrative Support** – Can provide non-accountable DTS support to command and **will not** approve or certify any payment (reimbursable/non-reimbursable) or initiate debt collections on behalf of any DTS traveler.
 - **CBA Specialist** – Can provide non-accountable DTS support to reconcile monthly CBA invoices and **will not** certify invoices for payment.
 - **Non-Approving Routing Official (RO)** – Can provide non-accountable DTS support to command in a routing list by applying any DTS routing stamp other than APPROVED.
 - **Travel Clerk/Preparer & Non-DTS Entry Agent (NDEA)** – Can provide non-accountable DTS support to command to prepare and sign Authorizations, Local Vouchers and Vouchers on behalf of another DTS traveler with required documentation as necessary (e.g. signed 1351-2 from traveler for Voucher payment)
 - **DTS Auditor/Travel Researcher** – See below
 - **Compliance Tool Administrator** – See below
 - **ROA Administrator** – See below
- ❖ **DTS Auditor/Travel Researcher** - May have a DTS user profile created with only permission level 0 and can be granted Read Only Access (ROA) in the Area of Responsibility (AOR) using a ROA Request Form submitted to MAJCOM LDTA.

- ❖ **Compliance Tool Administrator (CTA)** – CTAs must have a Passport/TraX account established to gain access to the CTA module. Access will be granted to the MAJCOM LDТА by the Navy DTS PMO. They will review records and errors, ensure errors are corrected, run reports from the CT, distribute reports as necessary to sub-commands, and grant CT access to others.
- ❖ **Read Only Access (ROA) Administrator** – ROA Administrator access will be granted to MAJCOM LDТАs by the NAVY DTS PMO. ROA Administrators are to add, modify, and delete ROA Users. They may grant additional ROA Administration access to Command ODTAs as needed. Command ODTAs are to **only** grant ROA User access in AOR. Any additional ROA access must be requested by submitting a ROA REQUEST FORM to the Navy DTS PMO.
- ❖ **Approval Override** – Organizations will send requests for Approval Override via the MAJCOM LDТА to the Navy DTS PMO for consideration. Proper justification is required. Approval Override requires Group Access and a valid DD FORM 577 must be on file. The individual cannot be present on any routing list.
- ❖ **Self-Authorizing Official (AO)** – Individuals who previously traveled under blanket travel authorization/orders may be designated as self-authorizing officials. These individuals may act as their own AOs authorizing their own itineraries and travel arrangements. They may not, however, certify their own claims for payment or approve authorizations with advances and/or SPPs for disbursements. They shall be designated in writing and shall acknowledge in writing that they may not certify their own claims for payments or approve authorizations with advances and/or SPPs for disbursements.
- ❖ **Delegate-Authority** – Is prohibited for all Navy DTS users due to the inability for other users, other than the grantor, to remove the delegated authority. It also does not accurately show up on the routing list report for SOD tracking and enforcement purposes.

SOD COMPLIANCE REFERENCES:

1. **Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (Green Book), Design of Appropriate Types of Control Activities, Segregation of duties, 10.03:**
 “Segregation of duties Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event.”
2. **DoD 7000.14-R FMR Vol. 5, Ch.1, 010305.B:**
 “Separation of duties precludes errors or attempts at fraud or embezzlement from going undetected. Internal controls generally require a four-way separation of the contracting, receiving, voucher certification, and disbursing functions. Assign key duties such as certification of fund availability; contracting (obligating the Government); authorizing, approving, and recording transactions; issuing or receiving assets; certifying and making payments; preparing and signing checks; and reviewing or auditing payments to different individuals to minimize the risk of loss to the Government to the greatest extent possible.
 1. Do not assign DOs duties that create potential conflicts of interest (see Chapter 2, paragraph 020305).
 2. Separation of duties is not always practical or possible due to time constraints, manpower shortages, or the use of electronic systems. Commanders and DOs must be aware of situations where valid, long-standing separation of duties cannot be achieved, recognize that internal controls have been weakened as a result, and make every effort to mitigate the risks. For example, payments and collections through the Intra-governmental Payment and Collection system can occur outside the disbursing work center without weakening internal controls because the payee is always another Federal agency and recovery of an improper payment is assured, or financial systems which allow for adjustments to the data outside of the normal application include appropriate controls and audit trails for those adjustments. Other situations may require closer scrutiny. Report all situations of inability to separate appropriate responsibilities to the DO’s commander, with a request for a waiver and recommendations to mitigate the risks.”
3. **DoD 7000.14-R FMR Vol. 5, Ch.5, 050201.A:**
 “Based on the separation of duties principles cited in Chapter 1, subparagraph 010305.B, DOs, their deputies, and agents may neither be appointed as, nor appoint certifying officers for payments they will eventually make. See subparagraph 050301.B for conditions that may require deviation from normal separation of duties requirements.”
4. **DoDI 5154.31, Vol. 3, 0304:**
 “DTS users may serve in more than one DTS role provided that an adequate separation of duties is maintained in accordance with DoD FMR, Volume 5 and DoD Component guidance.”
5. **DoDI 5154.31, Vol. 3, 030401.A-1:**
 “AOs that are appointed as COs. These AOs may approve all types of DTS documents, so long as AOs follow separation-of-duties requirements.”
6. **DoDI 5154.31, Vol. 3, 030407.A-4.**
 “[LDТА’s] Verify that DTS user permission levels provide an appropriate separation of duties. In cases where a clear separation of duties is not possible, the circumstances must be reported in accordance with DoD FMR, Volume 5, Chapter 1.

7. NAVADMIN 393/11:

“IRT NAVAUDSVC/22JUN10/, The Naval Audit Service identified numerous Navy DTS Administrators with insufficient Separation of Duties (SoD) within DTS. Specifically, the individuals identified had DTS permission levels enabling them to create, review and approve travel authorizations and vouchers. Insufficient SoD potentially permits the creation and submission of erroneous travel claims and the alteration of system data without visible evidence.”

“All commands are directed to immediately review all personnel assigned DTS permission levels and eliminate conflicts with insufficient SoD. When reassigning permission levels to ensure compliance, personnel should be assigned to only one position.”

8. NAVSUPINST 4650.8, 6-F:

“Key duties and responsibilities need to be divided or separated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related aspects. No one individual should control all key aspects of a transaction or event.”

9. NAVY DTS BUSINESS RULES – DTS Roles and Responsibilities:

“Since individuals can perform multiple roles (i.e., BDTA & FDTA, or RO & AO/CO) within DTS, commands must ensure that DTS roles, permissions, and accesses are in compliance with NAVADMIN 393/11 and the Navy Rules for Permissions and Accesses to the Defense Travel System/SOD Matrix.”