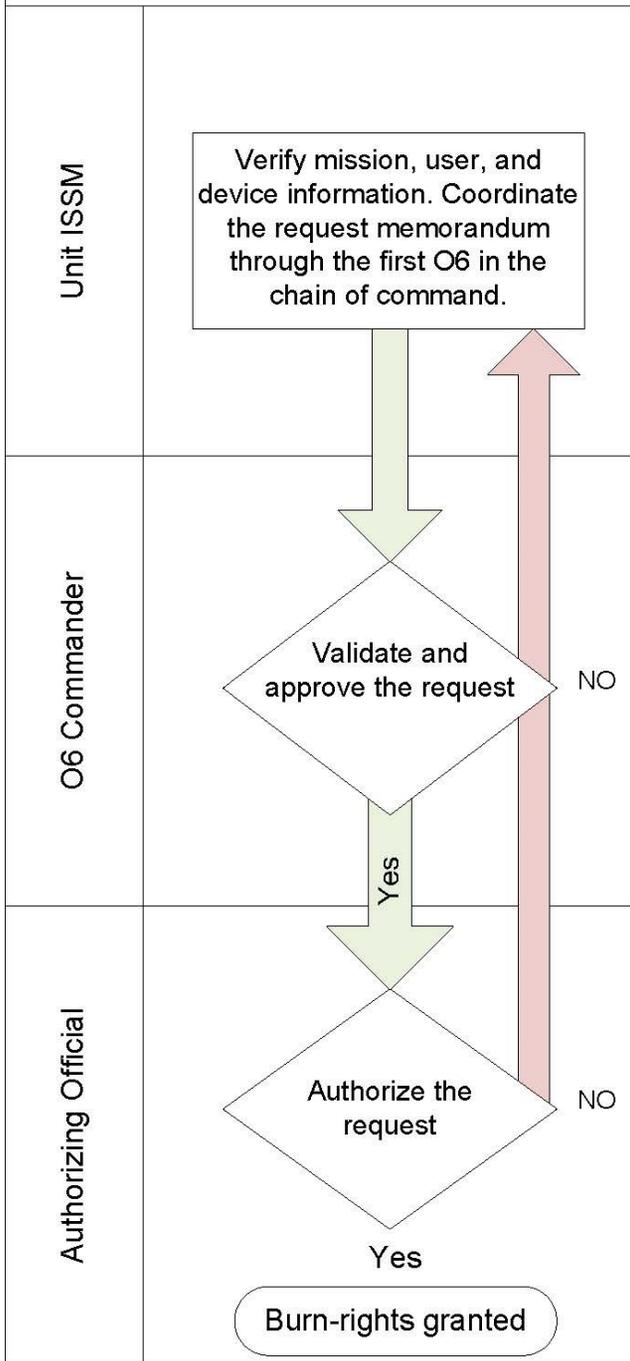


# DTA Request Process



iAssure Portal  
DTA Page

<http://go.usa.gov/ctjYm>



Army in Europe

DTA Program Management:

Policy, Programs, and Training (PP&T) Branch

Cybersecurity Division

USAREUR G6

E-mail: [usarmy.wiesbaden.usareur.mbx](mailto:usarmy.wiesbaden.usareur.mbx)

[g6-ia-ppt-branch@mail.mil](mailto:g6-ia-ppt-branch@mail.mil)

This publication is available at

<https://aepubs.army.mil>

AE MISC PUB 25-2F • 21 JUL 16



**Data Transfer Authority**





## What is Data Transfer Authority?

Data Transfer Authority (DTA) is a program that authorizes users the ability to burn information from the Secret Internet Protocol Router Network (SIPRNET) to removable media. This authorization will be granted only for valid functional requirements, not for personal convenience.

## What are common uses of DTA?

- Foreign disclosure operations
- IT-support operations
- Exercise operations

## What is removable media?

Removable media includes any type of storage device that can be removed from a computer while the system is running.

## Examples of removable media:

- Compact disks (CDs), digital versatile disks (DVDs), Blu-Ray disks
- External hard drives
- USB flash drives
- Tape drives
- Floppy drives

## What are the requirements for DTA?

1. A digitally signed DTA agreement.
2. Completed Personal Electronic Device (PED) v2.0 training.
3. A DTA memorandum.

## All DTA memorandums must include—

1. The requesting command's letterhead.
2. A justification for granting DTA.
3. The following system-identification information:
  - Name or identifier
  - Media access control (MAC) address
  - Serial number
  - Networked or stand-alone
4. A list of all users requiring authorization, providing the following information for each individual:
  - Full name
  - Grade or rank
  - Electronic data interchange personal identifier (EDIPI)
  - Military telephone number
  - E-mail address
5. Signatures of the following individuals in the order below:
  - a. Point of contact
  - b. Information system security manager (ISSM)
  - c. O6 or GS-15 at the major subordinate command
  - d. USAREUR authorizing official (AO)

A memorandum template is available on the iAssure DTA page at <http://go.usa.gov/ctjYm>.

## Users should be aware of the following:

- All data transfers must be logged.
- DTA log information must be submitted to the DTA logs SharePoint portal on SIPRNET iAssure.
- DTA permissions expire after 1 year. All users must resubmit requests annually to maintain their DTA authorizations.
- In the case of a new workstation (for example, because of life-cycle replacement), a new memorandum must be submitted for that device to obtain AO authorization.
- Allow 4 to 6 weeks for DTA requests to be approved.
- Do not use DTA permissions for anything outside the scope of what the AO has authorized.

## Additional information

- Ensure you follow all labeling and storage requirements when storing media that contains classified information.
- Never connect media containing classified information to the Nonsecure Internet Protocol Router Network (NIPRNET).
- Never leave devices or removable media with classified information unattended.
- Ensure proper destruction or disposal of removable media containing classified information.