Snapshot: Approval Paths for SAARs — External Users

Understanding Approval Paths

What is an "Approval Path"?

An Approval Path is a predefined workflow in AMPS that automates the process of approving various types of requests for approvers of the requests.

For Defense Logistics Agency (DLA) owned application roles, external approvers include the following staff members:

- **User-specified AMPS Supervisor (SUPV)**
- **User-specified Security Officer (SO)**
- **User-specified External Authorizing Official (EAO)**

What factors affect an Approval Path?

- **Type of request:** A Role Request, Role Removal, and Role Extension or Expiration have different paths. Role removal requests or expiration requests are reviewed by the Supervisor only.
- **Role Owning Organization** (DLA or DFAS)**: DLA roles do not require an IAO approval.** DFAS roles do require an IAO approval.
- **Position Sensitivity Levels** (Critical Sensitive (CS), Non-Critical Sensitive (NCS), or Non-Sensitive (NS))*: For External Users, the approval path is not affected by the user's Position Sensitivity or the requested role's Position Sensitivity.
  **Under the former "IT Level" nomenclature, CS = IT1, NCS = IT2, NS = IT3.*
- **Security Officer Bypass:** The SO participates in the approval process for all role requests made by External Users.
- **External Authorizing Official Reviews:** EAOs review role requests for specific EAO roles only (not shown).

External User Role Request for a DLA Role: Typical Approval Path

The diagram at right shows the approval path for an External User's request of a DLA role. (Role extension requests follow the same path and rules as the original request for the role.)

Factors:

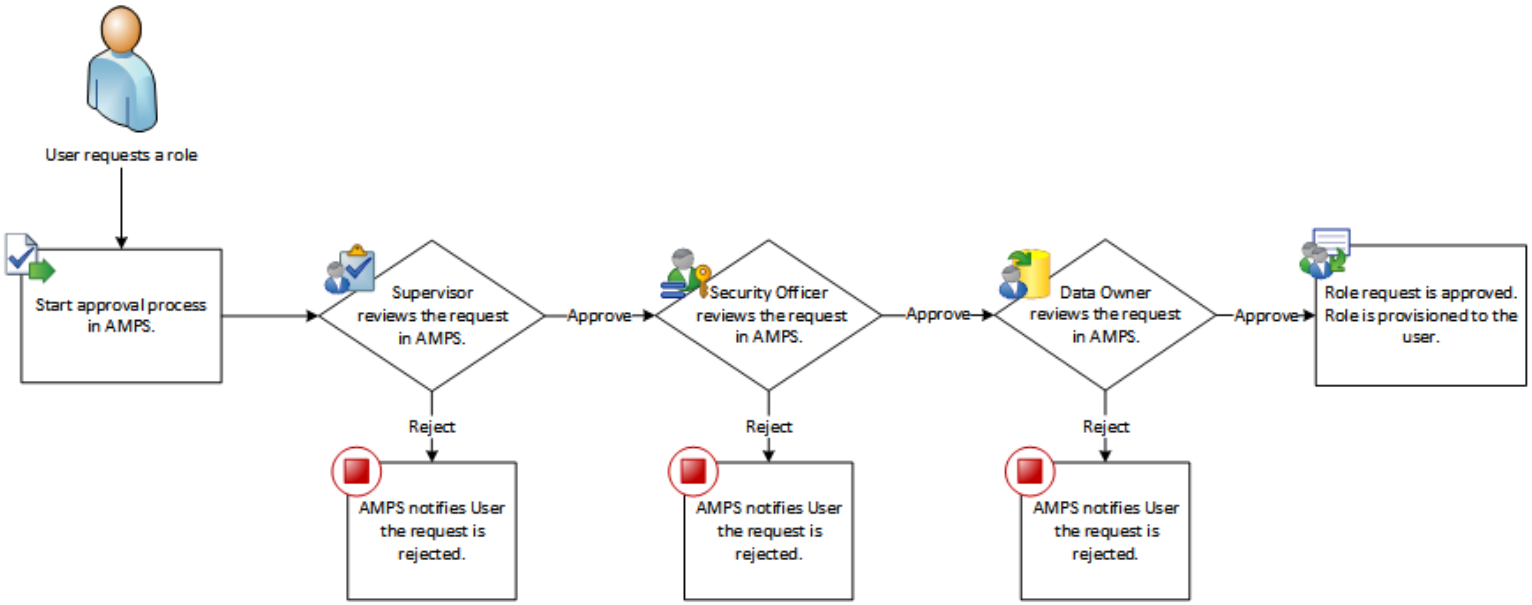
- Role is for an application owned by DLA.

Approvers:

- **Supervisor**
- **Security Officer**
- **Data Owner**

Rules:

- The Supervisor reviews every role request submitted by a user.
- The Security Officer is never bypassed on a role request from an External User.
- A Data Owner reviews every role request submitted by a user.



Property of U.S. Government, 2024. Approved for public release. Distribution unlimited.

Snapshot: Approval Paths for SAARs — External Users

Understanding Approval Paths

What is an "Approval Path"?

An Approval Path is a predefined workflow in AMPS that automates the process of approving various types of requests for approvers of the requests.

For Defense Finance and Accounting Service (DFAS) owned application roles, external approvers include the following staff members:

- **User-specified AMPS Supervisor (SUPV)**
- **User-specified Security Officer (SO)**
- **User-specified External Authorizing Official (EAO)**

What factors affect an Approval Path?

- **Type of request:** A Role Request, Role Removal, and Role Extension or Expiration have different paths. Role removal requests or expiration requests are reviewed by the Supervisor only.
- **Role Owning Organization** (DFAS or DLA)**: DFAS roles do require an IAO approval.** DLA roles do not require an IAO approval.
- **Position Sensitivity Levels** (Critical Sensitive (CS), Non-Critical Sensitive (NCS), or Non-Sensitive (NS))*: For External Users, the approval path is not affected by the user's Position Sensitivity or the requested role's Position Sensitivity.
  **Under the former "IT Level" nomenclature, CS = IT1, NCS = IT2, NS = IT3.*
- **Security Officer Bypass:** The SO participates in the approval process for all role requests made by External Users.
- **External Authorizing Official Reviews:** EAOs review role requests for specific EAO roles only (not shown).

External User Role Request for a DFAS Role: Typical Approval Path

The diagram at right shows the approval path for an External User's request of a DFAS role. (Role extension requests follow the same path and rules as the original request for the role.)

Factors:

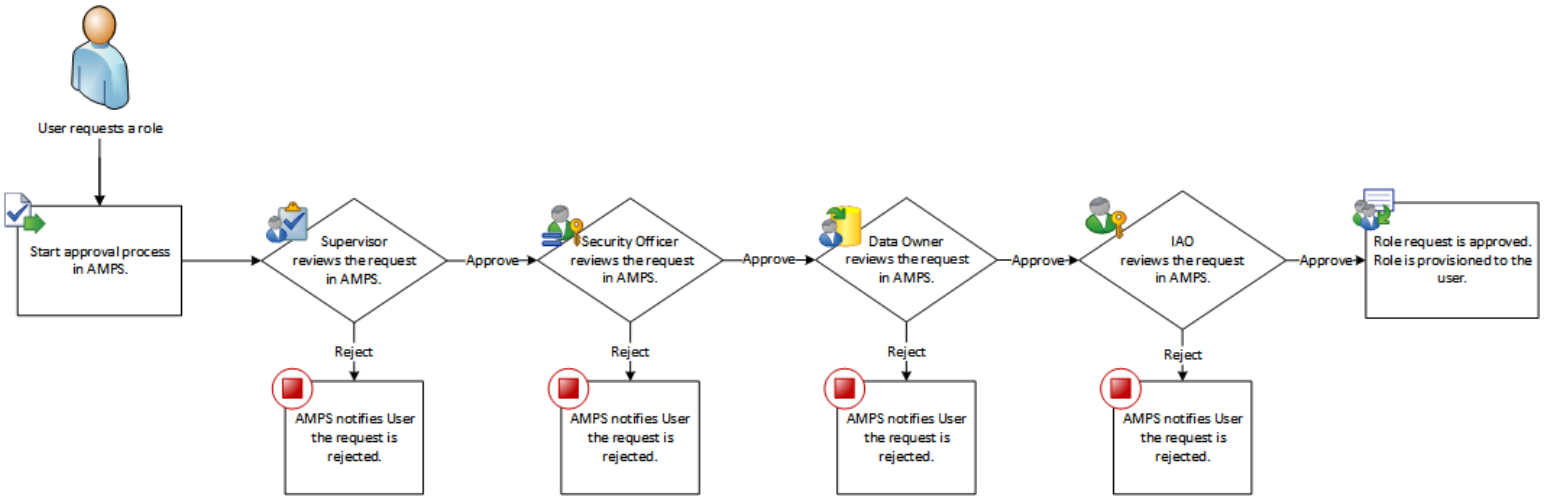
- Role is for an application owned by DFAS.

Approvers:

- **Supervisor**
- **Security Officer**
- **Data Owner**
- **Information Assurance Officer**

Rules:

- The Supervisor reviews every role request submitted by a user.
- The Security Officer is never bypassed on a role request from an External User.
- A Data Owner reviews every role request submitted by a user.
- An Information Assurance Officer approval is required for all DFAS role requests.



Property of U.S. Government, 2024. Approved for public release. Distribution unlimited.

Snapshot: Approval Paths for SAARs — External Users

Understanding Approval Paths

What is an "Approval Path"?

An Approval Path is a predefined workflow in AMPS that automates the process of approving various types of requests for approvers of the requests.

In AMPS, external approvers include the following staff members:

- **User-specified AMPS Supervisor (SUPV)**
- **User-specified Security Officer (SO)**
- **User-specified External Authorizing Official (EAO)**

What factors affect an Approval Path?

- **Type of request:** A Role Request, Role Removal, and Role Extension or Expiration have different paths. Role removal requests or expiration requests are reviewed by the Supervisor only.
- **Role Owning Organization** (DLA or DFAS)**:** Neither organization requires an IAO approval for role removals.
- **Position Sensitivity Levels** (Critical Sensitive (CS), Non-Critical Sensitive (NCS), or Non-Sensitive (NS))*: For External Users, the approval path is not affected by the user's Position Sensitivity or the requested role's Position Sensitivity.
  **Under the former "IT Level" nomenclature, CS = IT1, NCS = IT2, NS = IT3.*
- **Security Officer Bypass:** The SO participates in the approval process for all role requests made by External Users.
- **External Authorizing Official Reviews:** EAOs review role requests for specific EAO roles only (not shown).

Role Removal or Role Expiration Request: Typical Approval Path

The diagram at right shows the approval path for a user's role removal or role expiration request.

Factors:

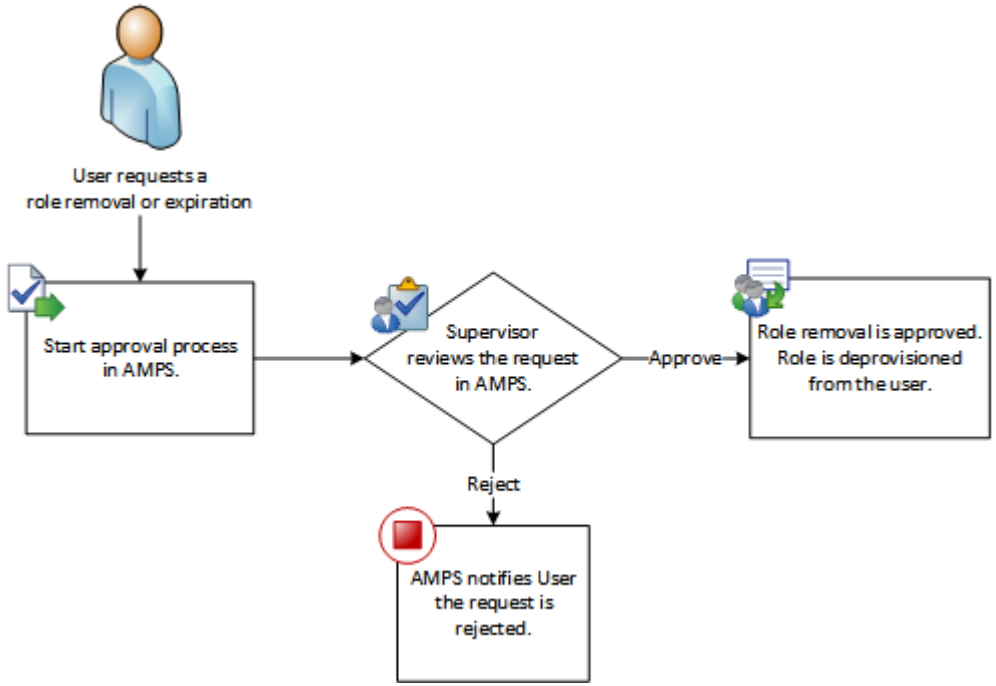
- Role removal (or expiration) vs. role request.

Approvers:

- **Supervisor**

Rules:

- The Supervisor reviews every role request submitted by a user, including role removal and expire requests.
- Security Officers, Data Owners, and Information Assurance Officers do not review role removal or role expiration requests.



Property of U.S. Government, 2024. Approved for public release. Distribution unlimited.