OR-003f — Cross-Domain Transfer Control

Go to OR-003 — Classified and Unclassified Environments

Statement

Crucible SHALL transfer information between Security Domains only through an authorized Cross-Domain Transfer.

Derived From

This requirement derives from:

- OR-003 — Classified and Unclassified Environments
- Crucible System Requirements Specification, Version 1.1 Draft, Operational Requirements, OR-003

The Original Requirement states:

> *The system SHALL support classified and unclassified deployment environments.*[C1]

OR-003f isolates the obligation to control information movement between Security Domains.

Rationale

Authorization to process information within one Security Domain does not authorize movement of that information into another Security Domain.

A transfer can cross boundaries established by different security policies, classification levels, compartments, handling restrictions, organizations, missions, or release authorities.

OR-003f prevents Crucible from moving information across a Security Domain boundary without an authorized Cross-Domain Transfer.

The Crucible Concept of Operations describes dependency capture, transfer-bundle creation, import, validation, and offline use across connected, disconnected, and air-gapped environments.

When the source and destination environments belong to different Security Domains, that workflow constitutes a Cross-Domain Transfer and requires the controls established by OR-003f.

Applies To

This requirement applies to:

- Crucible
- Security Domains
- Cross-Domain Transfers
- Information transferred by Crucible
- Artifacts
- Machine Images
- Infrastructure Baselines
- Crucible Descriptions
- Dependencies
- Evidence
- Classified Environments
- Unclassified Environments
- Connected Environments
- Disconnected Environments
- Air-Gapped Environments

Verification

Verification confirms that:

1. Each tested transfer identifies its source Security Domain
2. Each tested transfer identifies its destination Security Domain
3. Each tested transfer identifies the information selected for transfer
4. Each tested transfer identifies an authorized Cross-Domain Transfer
5. Crucible transfers the selected information when the Cross-Domain Transfer is authorized
6. Crucible prevents the transfer when the Cross-Domain Transfer is not authorized
7. Crucible prevents the transfer when the source Security Domain is not identified
8. Crucible prevents the transfer when the destination Security Domain is not identified
9. Crucible records the result of each attempted Cross-Domain Transfer
10. Each transfer record identifies the source Security Domain, destination Security Domain, transferred information, transfer authorization, and transfer result

Referenced By

The following pages reference this requirement:

- 3.3 Security Domains and Transfer Boundaries
- 4.1 Human Actors
- 7.3 Transfer Across the Boundary
- 7.4 Import the Transfer Bundle
- Annex D: Requirements Traceability

Delivery Phase

Implemented and Verified.

Implementation Status

☐ Assess whether the current Crucible implementation transfers information between Security Domains only through an authorized Cross-Domain Transfer.

Requirement Status

☐ Review and approve OR-003f as a leaf requirement derived from OR-003.

Issues

☐ Identify the authority responsible for authorizing each supported Cross-Domain Transfer.

☐ Define how Crucible identifies the source Security Domain.

☐ Define how Crucible identifies the destination Security Domain.

☐ Define how Crucible identifies the information selected for transfer.

☐ Define how Crucible determines whether a Cross-Domain Transfer is authorized.

☐ Define the behavior required when the source and destination belong to the same Security Domain.

☐ Define the behavior required when the source or destination Security Domain cannot be determined.

☐ Define the record required for an authorized, denied, failed, or terminated Cross-Domain Transfer.

Notes for Editors

This requirement page should retain the stable requirement identifier `OR-003f`.

This page is a leaf requirement page and omits a trailing `:start` from its namespace.

OR-003f governs whether information may cross a Security Domain boundary. It does not define the detailed processing steps performed by a Cross-Domain Transfer mechanism.

The responsible authority establishes:

- The authorized source Security Domain
- The authorized destination Security Domain
- The information authorized for transfer
- The authorized transfer mechanism
- The transfer direction
- The conditions governing transfer authorization
- The evidence required to demonstrate authorization

Changes to the Statement should preserve:

- Crucible as the responsible actor
- Transfer as the controlled behavior
- Information as the transferred object
- Distinct Security Domains as the source and destination contexts
- An authorized Cross-Domain Transfer as the required transfer path

Requirements governing whether information is authorized within a Security Domain should remain in OR-003d — Security Domain Information Enforcement.

Requirements governing the permitted handling of information should remain in OR-003e — Information Handling Rule Enforcement.

To reference this requirement Statement from another wiki page, insert:

```
{{section>dido:02-crusible:99-annexes:annex-c-requirements:02-operational-requirements:or-003:or-003f#Statement&noheader&nofooter&noeditbtn}}
```

Do not rename this page after an external citation unless a redirect or move plan is in place.
