

7.3 Transfer Across the Boundary

[Go to 7. Disconnected and Air-Gapped Operations](#)

The transfer activity moves an authorized [Transfer Bundle](#) from its source [Security Domain](#) across a controlled boundary toward the destination environment.

The applicable organization controls the transfer through its approved personnel, procedures, media, transfer services, and cross-domain mechanisms. [Crucible](#) provides the identified Transfer Bundle and the information required to associate the transferred content with the applicable lifecycle activity.

Producing a Transfer Bundle does not authorize its release or movement across the boundary.

Identify the Transfer Boundary

The transfer activity identifies the boundary separating the source environment from the destination environment.

The boundary can separate:

- A Connected Environment from a Disconnected Environment
- A Connected Environment from an Air-Gapped Environment
- Two Security Domains
- Two environments governed by different information-handling rules
- Two environments with different access restrictions
- An export environment from an import environment

The governing organization determines the controls and approvals applicable to the identified boundary.

Identify the Transfer Bundle

The transfer activity uses the Transfer Bundle produced in [7.2 Produce the Transfer Bundle](#).

The bundle remains identifiable throughout the transfer process.

The transfer information can identify:

- The Transfer Bundle identifier
- The source environment
- The destination environment
- The source Security Domain
- The destination Security Domain
- The planned destination activity
- The bundle-production result
- Available integrity information
- The applicable handling restrictions

The transfer process must not substitute an unidentified or modified bundle for the approved Transfer Bundle.

Apply Information-Handling Rules

The applicable information-handling rules govern whether the Transfer Bundle can cross the identified boundary.

Those rules can restrict:

- The information permitted in the bundle
- The source from which the information originates
- The destination permitted to receive the information
- The transfer mechanism
- The personnel authorized to perform or approve the transfer
- The media permitted for the transfer
- The required inspection or review
- The required integrity protection
- The records required for the transfer

Crucible does not override an information-handling restriction or convert an unauthorized transfer into an authorized transfer.

Enforce Cross-Domain Transfer Control

Cross-domain transfer control applies the rules governing movement between the source and destination Security Domains.

The control decision can permit, deny, or prevent the transfer according to the applicable policy and authorization.

A permitted transfer establishes only that the approved transfer process allows the identified bundle to proceed across the boundary. It does not establish that:

- The destination accepts the bundle
- The bundle imports successfully
- The included content is suitable for every destination activity
- The destination environment satisfies applicable compliance criteria
- The transferred content receives operational approval

Separate import, verification, assessment, deployment, and authorization activities make those determinations.

Use an Approved Transfer Mechanism

Authorized personnel use an organization-approved transfer mechanism to move the Transfer Bundle.

The approved mechanism can include:

- Controlled removable media
- An approved transfer service
- A cross-domain solution
- A controlled staging environment
- Another authorized physical, logical, or procedural mechanism

The governing organization determines which mechanism is appropriate for the boundary and the information being transferred.

Crucible does not define or replace the organization's media-control, chain-of-custody, release, inspection, or cross-domain authorization procedures unless an applicable requirement explicitly assigns that behavior to Crucible.

Protect Bundle Integrity

The transfer process maintains the identity and integrity information associated with the Transfer Bundle.

Integrity verification can compare the transferred bundle with the value recorded when Crucible produced the bundle.

An integrity mismatch indicates that the received bundle does not correspond to the expected bundle representation.

A successful integrity verification does not independently establish that the transfer complied with every organizational or regulatory requirement.

Record the Transfer Result

The transfer result can identify:

- The Transfer Bundle transferred
- The source environment
- The destination environment
- The applicable Transfer Boundary
- The transfer mechanism
- The transfer status
- The transfer time
- The integrity information
- Any denial, interruption, or unresolved condition

The organization's approved transfer process determines any additional custody, release, inspection, transport, receipt, or accountability records.

The transferred bundle becomes the controlled input to [7.4 Import the Transfer Bundle](#).

Requirements Addressed

Requirement	Statement
OR-003d — Security Domain Information Enforcement	Crucible SHALL prevent an operation from processing information not authorized within the operation's governing Security Domain .
OR-003e — Information Handling Rule Enforcement	Crucible SHALL prevent an operation from handling information in a manner prohibited by the Information Handling Rules governing that information.
OR-003f — Cross-Domain Transfer Control	Crucible SHALL transfer information between Security Domains only through an authorized Cross-Domain Transfer .

The linked leaf requirement pages remain the canonical sources.

© 2026 Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

From:
<https://wiki.didosolutions.com/> - **Dido Solutions, Inc Wiki**

Permanent link:
<https://wiki.didosolutions.com/dido/02-crucible/07-disconnected-and-air-gapped-operations/07-03-transfer-across-the-boundary>

Last update: **2026/08/01 07:06**

