OR-003d — Security Domain Information Enforcement

Go to OR-003 — Classified and Unclassified Environments

Statement

Crucible SHALL prevent an operation from processing information not authorized within the operation's governing Security Domain.

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-003d isolates the obligation to prevent a Crucible operation from processing information outside the authorization boundary of its governing Security Domain.

Rationale

A Classified Environment or Unclassified Environment can contain information governed by different Security Domains.

Execution within an authorized environment does not by itself authorize an operation to process all information present or accessible within that environment.

OR-003d prevents a Crucible operation from processing information outside the information boundary established for its governing Security Domain.

The responsible authority establishes the Security Domain and identifies the information authorized within it. Crucible enforces the established authorization.

Applies To

This requirement applies to:

- Crucible
- Crucible operations
- Security Domains
- Information processed by Crucible operations
- Classified Environments
- Unclassified Environments

Verification

Verification confirms that:

1. Each tested Crucible operation identifies its governing Security Domain
2. The governing Security Domain identifies the information authorized within the domain
3. Crucible permits the tested operation to process information authorized within the governing Security Domain
4. Crucible prevents the tested operation from processing information not authorized within the governing Security Domain
5. Crucible records each denial caused by a Security Domain information restriction
6. Each denial record identifies the operation, governing Security Domain, requested information, and denial result

Referenced By

The following pages reference this requirement:

- 3.3 Security Domains and Transfer Boundaries
- 4.1 Human Actors
- 4.3 External Systems
- 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 prevents each operation from processing information not authorized within its governing Security Domain.

Requirement Status

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

Issues

☐ Identify the authority responsible for establishing each Security Domain used by Crucible.

☐ Define how each Crucible operation identifies its governing Security Domain.

☐ Define how each Security Domain identifies the information authorized within the domain.

☐ Define how Crucible determines the Security Domain associated with information.

☐ Define the behavior required when an operation does not identify a governing Security Domain.

☐ Define the behavior required when information does not identify an associated Security Domain.

☐ Define the record required when Crucible denies information processing because of a Security Domain restriction.

Notes for Editors

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

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

OR-003d requires enforcement of an established Security Domain information boundary. It does not require Crucible to establish, authorize, or define a Security Domain.

The responsible authority establishes:

- The Security Domain identifier
- The Security Domain boundary
- The governing security policy
- The information authorized within the Security Domain

Changes to the Statement should preserve:

- Crucible as the responsible actor
- Prevention as the required behavior
- A Crucible operation as the subject of enforcement
- Information as the controlled object
- The governing Security Domain as the source of authorization

Requirements governing access to resources should remain in OR-003c — Security Domain Resource Enforcement.

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

Requirements governing movement of information between Security Domains should remain in OR-003f — Cross-Domain Transfer Control.

Requirements governing user or process authorization should remain in OR-003g — Security Domain Access Control.

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-003d#Statement&noheader&nofooter&noeditbtn}}
```

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