Cross-Domain Transfer

Go up to Terms and Definitions

Discussion

A Cross-Domain Transfer is the controlled movement of information or an information-bearing Artifact from one Security Domain to another Security Domain.

The source and destination Security Domains can differ in:

- Security Classification
- Compartments
- Handling caveats
- Dissemination restrictions
- Security policy
- Authorization authority
- Mission purpose
- Organizational control
- Connectivity
- Information-release policy
- Trust level

A Cross-Domain Transfer can move information:

- From a lower-classification domain to a higher-classification domain
- From a higher-classification domain to a lower-classification domain
- Between domains at the same classification level
- Between classified and unclassified domains
- Between compartments
- Between organizations
- Between Connected, Disconnected, or Air-Gapped Environments

A transfer between domains at the same Security Classification remains a Cross-Domain Transfer when different security policies, compartments, authorities, or release rules govern the domains.

A Cross-Domain Transfer can use:

- An authorized Cross-Domain Solution
- A high-assurance guard
- A controlled file-transfer mechanism
- Approved removable media
- A manual review and release process
- An authorized import or export service
- A controlled repository-transfer process
- An approved physical transfer process

A Cross-Domain Transfer can include:

- Identification of the source Security Domain
- Identification of the destination Security Domain
- Identification of the information or Artifact
- Validation of the Security Classification
- Validation of markings and metadata
- Evaluation of Information Handling Rules
- Authorization of the transfer
- Content inspection
- Malware inspection
- File-type validation
- Format transformation
- Metadata filtering
- Content filtering
- Redaction
- Downgrading or release review
- Transfer execution
- Receipt confirmation
- Transfer Evidence generation
- Provenance preservation
- Traceability preservation

Transfer from a higher-classification domain to a lower-classification domain requires an authorized release, downgrading, declassification, sanitization, or review process. The transfer mechanism does not itself grant authority to release the information.

Transfer into a higher-classification domain can also require validation because imported information or software can introduce:

- Malicious content
- Unauthorized Dependencies
- Unapproved executable code
- Invalid metadata
- Incorrect markings
- Supply-chain risk
- Configuration inconsistency

Within Crucible, Cross-Domain Transfer can apply to:

- Crucible Descriptions
- Infrastructure Baselines
- Machine Images
- Software packages
- Dependencies
- Configuration data
- Deployment records
- Validation results
- Evidence
- Updates
- Provider Implementations

Definition

controlled movement of information or an information-bearing Artifact from one Security Domain to another

Source

- Committee on National Security Systems Instruction 4009, Committee on National Security Systems Glossary
- NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations
- NIST Special Publication 800-160 Volume 1, Engineering Trustworthy Secure Systems
- Dido Solutions, Crucible architecture and requirements terminology

Note

A Cross-Domain Transfer is not equivalent to ordinary network transmission.

The transfer must account for the security policies and Information Handling Rules of both the source and destination Security Domains.

A Cross-Domain Transfer can occur without a direct network connection. For example, approved removable media can carry information between two Air-Gapped Environments.

A Cross-Domain Solution is a technical or procedural mechanism used to perform or control a Cross-Domain Transfer. The solution and the transfer are distinct:

- The Cross-Domain Solution is the mechanism
- The Cross-Domain Transfer is the controlled movement

A successful technical transfer does not establish that the transfer was authorized or compliant. The transfer record must demonstrate satisfaction of the governing Information Handling Rules.

Example

A Crucible Infrastructure Baseline moves from a Connected Unclassified Environment to an Air-Gapped Classified Environment.

The Cross-Domain Transfer process:

- Identifies the source and destination Security Domains
- Confirms that the Infrastructure Baseline is authorized for import
- Validates the Artifact identifiers and revisions
- Verifies digital signatures and integrity values
- Scans the files for malicious content
- Confirms that all Dependencies are authorized

- Removes prohibited metadata
- Transfers the files using approved media
- Validates the transferred content in the destination domain
- Records the transfer authority, date, source, destination, results, Evidence, Provenance, and Traceability

---