Security Classification

Go up to Terms and Definitions

Discussion

A Security Classification is a designation assigned by an authorized classification authority to information whose unauthorized disclosure could cause a defined degree of harm.

The Security Classification identifies the protection level and handling controls required for the information.

A classification framework can define:

- Classification levels
- Classification markings
- Original classification authorities
- Derivative classification rules
- Classification duration
- Downgrading rules
- Declassification rules
- Access requirements
- Need-to-know requirements
- Storage requirements
- Transmission requirements
- Reproduction restrictions
- Dissemination restrictions
- Media-handling requirements
- Destruction requirements
- Incident-reporting requirements

Within the United States national security classification system, the principal classification levels are:

- Confidential
- Secret
- Top Secret

Other national, multinational, military, intelligence, and organizational classification frameworks can use different levels, names, markings, and handling requirements.

A Security Classification can be accompanied by additional controls, including:

- Compartments
- Special access restrictions
- Dissemination controls
- Nationality restrictions
- Handling caveats
- Mission restrictions

- Releasability markings

A Security Classification can apply to:

- Information
- Documents
- Data records
- Messages
- Files
- Artifacts
- Machine Images
- Infrastructure Baselines
- Configuration records
- Deployment records
- Evidence
- Metadata
- Aggregations of information

An environment does not acquire a Security Classification merely because classified information might be relevant to its mission. The responsible authority must authorize a Classified Environment to handle information at specified classification levels and under specified handling restrictions.

Within the Crucible architecture, the Security Classification associated with a Deployment Target can constrain:

- The Infrastructure Baselines permitted for deployment
- The Machine Images permitted for deployment
- The Artifacts permitted within the environment
- The Dependency Stores available to the environment
- The users and roles permitted to perform Deployment Operations
- The information-transfer mechanisms
- The Provider Implementation
- The required security controls
- The required validation and Evidence
- The permitted connections to other environments

Definition

designation assigned by an authorized authority to information to identify the degree of protection required against unauthorized disclosure

Source

- Executive Order 13526, Classified National Security Information
- 32 CFR Part 2001, Classified National Security Information
- Dido Solutions, Crucible architecture and requirements terminology

Note

Security Classification is not the same as security categorization.

Security Classification primarily addresses protection against unauthorized disclosure under a classification authority.

Security categorization commonly evaluates potential impact to:

- Confidentiality
- Integrity
- Availability

A system can therefore be:

- Unclassified and categorized as high impact
- Classified and categorized according to a separate impact framework
- Authorized for one Security Classification but not another
- Authorized for a classification level but not for every compartment or handling caveat associated with that level

Controlled Unclassified Information is not a Security Classification. It is unclassified information subject to safeguarding or dissemination controls.

A Security Classification assigned to information remains in effect until an authorized action changes or removes the classification.

Example

An Infrastructure Baseline has the Security Classification **Secret** because its configuration, topology, and mission-specific controls contain classified information.

Crucible permits Deployment of the Infrastructure Baseline only to a Deployment Target whose record identifies:

- Authorization for Secret information
- Authorization for the required compartments and handling caveats
- Approved users and administrative roles
- Approved Machine Images and Dependencies
- Required storage and transmission protections
- Required audit and monitoring controls
- Required information-transfer procedures
- Required Evidence and Traceability
