

Classified Environment

[Go up to Terms and Definitions](#)

Discussion

A Classified Environment is an operating environment authorized to store, process, or transmit information assigned a [Security Classification](#).

The authorization for a Classified Environment identifies the classifications and additional handling restrictions that the environment can support.

A Classified Environment can include controls for:

- Physical access
- Personnel access
- Identity and authentication
- Authorization
- Information marking
- Information storage
- Information transmission
- Cryptographic protection
- Network separation
- Media handling
- Import and export of information
- Audit logging
- Continuous monitoring
- Configuration management
- Incident response
- Information retention
- Information destruction
- Equipment maintenance
- Hardware and software supply-chain controls

A Classified Environment can operate as a:

- [Connected Environment](#)
- [Disconnected Environment](#)
- [Air-Gapped Environment](#)

Connectivity and classification describe different environment characteristics:

- Connectivity describes the environment's access to external networks and resources
- Security Classification describes the information the environment is authorized to handle

An Air-Gapped Environment is not necessarily a Classified Environment. An Air-Gapped Environment becomes a Classified Environment only when the responsible authority authorizes it to handle classified information.

A Classified Environment can impose additional restrictions based on:

- Classification level
- Compartments
- Special access programs
- Dissemination controls
- Nationality restrictions
- Mission restrictions
- Need-to-know determinations
- Handling caveats
- Governing security policy

Within the Crucible architecture, a Classified Environment can contain one or more [Deployment Targets](#). Each Deployment Target record should identify the Security Classifications and handling restrictions authorized for that target.

Definition

operating environment authorized to store, process, or transmit information assigned one or more specified Security Classifications

Source

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

Note

A Classified Environment is authorized for specified Security Classifications. Authorization for one classification does not automatically authorize the environment for a higher classification, a different compartment, or an additional handling restriction.

A Classified Environment can also contain unclassified information when governing policy permits the information to enter and remain within the environment.

The term does not identify a specific national classification framework. Each organization or governing authority defines its classification levels, markings, handling controls, and authorization process.

A Classified Environment differs from an [Unclassified Environment](#):

- A Classified Environment is authorized to handle specified classified information
- An Unclassified Environment is not authorized to handle classified information

Example

A Deployment Target operates within an Air-Gapped Environment authorized to process information classified at the Secret level.

The Deployment Target record identifies:

- Secret as the maximum authorized Security Classification
- The permitted compartments and handling caveats
- The approved users and roles
- The authorized software and Machine Images
- The authorized Dependency Stores
- The media-transfer procedures
- The monitoring and audit requirements
- The information-retention and destruction requirements

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

From:

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

Permanent link:

https://wiki.didosolutions.com/dido/99_annexes/annex-b-terms-and-definitions/c/classified_environment

Last update: **2026/07/22 13:21**

