

# LEXICON GUIDE

## TERMS

**Access Solution** - CDS that provides simultaneous visual access to multiple security domains via a single workstation.

**Authorizing Official** - Senior agency principal with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

**Boundary Protection** - Monitoring and control of communications at the border of an information system to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).

**Centralized Service** - An application service provided by one organization either at one central facility or at distributed locations.

**Common Security Control** - Security control that can be applied to one or more agency information systems and has the following properties: the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and the results from the assessment of the control can be used to support the security certification and approval to operate processes of an agency information system where that control has been applied.

**Community of Interest** - A restricted, collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who, therefore, must have a shared vocabulary for the information they exchange. The group exchanges information within and between systems to include security domains.

**Controlled Interface** - A set of mechanisms that enforce the security policies and control the flow of information between interconnected information systems.

**Cross Domain Baseline** - CD mechanisms that are available for further deployment and reuse. These mechanisms are supported by the body of evidence necessary to make an accreditation decision.

**Cross Domain Capability** - The set of functions that enable the transfer of information between security domains in accordance with the policies of the security domains involved. Transfer includes the concept of Access when the information is not stored locally after transfer.

**Cross Domain Of cer** - Position, possibly within the Cross Domain Support Of ce, that serves as the validation of official for the organization.

**Cross Domain Solution** - A form of controlled interface that provides the capability to manually and/or automatically access and/or transfer information between different security domains and enforce their security policies.

**Cross Domain Support Of ce** - An organization responsible for coordinating CD requests with the UCDMO.

**Data Transfer Solution** - CDS that interconnects networks or information systems that operate at different security domains and transfers information between them.

**Enclave** - Collection of IS(s) connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

**Enterprise Architecture** - Explicit description and documentation of the current and desired relationships among business and management processes and IT.

**Enterprise Risk Management** - The management of the portfolio of risks to the organization's missions and existence (i.e., risks that the enterprise cannot adequately accomplish its current missions as well as risks that the enterprise will be unable to accomplish its future missions) and viability risks (i.e., risks that the enterprise will be terminated or its performance greatly reduced.)

**Enterprise Service** - A heterogeneous aggregation of multiple services that provides cross-application activities, spans disparate applications, and crosses organizational boundaries.

**Gateway** - Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.

**Guard** - A mechanism that mediates the exchange of information between information systems or subsystems.

**High Assurance Guard** - An enclave boundary protection device that controls access between a network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

**High Impact** - The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

**Information Domain** - A three-part concept for information sharing, independent of, and across information systems and security domains that:

Identifies information sharing participants as individual members,  
Contains shared information objects, and  
Provides a security policy that identifies the roles and privileges of the members and the protections required for the information objects.

**Information Sharing** - The requirements for information exchange by an IT system with one or more other IT systems or applications, for information exchange to support multiple internal or external organizations, missions, or public programs.

**Information Sharing Environment** - An approach that facilitates the exchange of information and which may include any methods determined necessary and appropriate.

**IT Governance Process** - The business process required by an organization to demonstrate its management of IT investments.  
**Low Impact** - The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

**Moderate Impact** - The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

**Multi-level Security** - Concept of processing information with different classification and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.

**Multiple Level Solution** - CD solution used to store data in multiple security domains that allows users to access the data at an appropriate security level.

**Mutual Authentication** - Occurs when parties at both ends of a communication activity authenticate each other.

**National Security Information** - Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the



