

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Accreditation Boundary. Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged.

E2.1.2. Accreditation Decision. An official designation from a DAA, in writing or digitally signed and made visible to the DoD CIO, regarding acceptance of the risk associated with operating a DoD information system and expressed as an Authorization to Operate (ATO), an Interim Authorization to Operate (IATO), an Interim Authorization to Test (IATT), or a Denial of Authorization to Operate (DATO).

E2.1.3. Adequate Security. Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that DoD information systems operate effectively and provide appropriate confidentiality, integrity, and availability, through implementation of assigned IA Controls. The DoD methodology for determining assigned IA Controls is defined in DoDD 8500.1 and the baseline DoD management, personnel, operational, and technical IA Controls are established in DoDI 8500.2.

E2.1.4. Artifacts. System policies, documentation, plans, test results and the like that express or enforce the IA posture of the DoD information system, make up the C&A information, and provide evidence of compliance with the assigned IA Controls.

E2.1.5. Assigned IA Controls. A list of IA Controls that a DoD information system must address to achieve an adequate IA posture. Assigned IA Controls include baseline DoD IA Controls, optional DoD IA Controls for special conditions or technologies, e.g., health information portability and privacy or cross security domain solutions, and DoD, Mission Area, Component and DoD information system supplements, if any. DoDI 8500.2.

E2.1.6. Authorization Termination Date (ATD). The date assigned by the DAA that indicates the date upon which authorization to operate is terminated for an ATO, IATO, or IATT.

E2.1.7. Authorization to Operate (ATO). The authorization, granted by a DAA, for a DoD information system to process, store, or transmit information. Authorization is based on acceptability of the IA component, the system architecture and implementation of assigned IA Controls.

E2.1.8. Automated Information System (AIS) Application. See DoD Information System.

E2.1.9. Certification. A comprehensive validation of actual IA capabilities and services of a DoD information system, made as part of and in support of the DIACAP, to establish compliance with assigned IA Controls based on standardized procedures.

E2.1.10. Certification Determination. A CA's validation of the system's compliance with IA controls, identifying and assessing the risks with operating the system, and the cost to correct or mitigate the IA security weakness.

E2.1.11. Certifying Authority (CA). The senior official having the authority and responsibility for the certification of information systems governed by a DoD Component IA Program.

E2.1.12. Certifying Authority Representative. Official acting on behalf of the Certifying Authority

E2.1.13. Communities of Interest (COI). An inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their

## Untitled

shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. Communities of Interest in the DoD can be either institutional or expedient. Institutional COIs whether functional or cross-functional, tend to be continuing entities with responsibilities for ongoing operations. Expedient COIs are more transitory and ad hoc, focusing on contingency and crisis operations. DoD Net-Centric Data Strategy", (reference (n)) addresses institutional and expedient COIs.

E2.1.14. Confidentiality Level (CL). Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-share determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The DoDI 8500.2 defines three confidentiality levels: classified, sensitive, and public.

E2.1.15. Core Enterprise Services (CES). A set of common services intended to provide or improve access, enable information sharing, and enhance interoperability among GIG entities. Core Enterprise Services enable service oriented architectures and may include web services. Examples of CES include enterprise management, messaging, discovery, mediation, collaboration, hosting, storage, IA/security, and user assistance.

E2.1.16. Defense and Intelligence Community Accreditation Support Team (DICAST). Facilitates the joint management of risk brought about by interconnecting the networks of the DoD and Intelligence Community Components.

E2.1.17. Defense IA/Security Accreditation Working Group (formerly DISN Security Accreditation Working Group). The DSAWG develops and provides accreditation recommendations to the PAAs, DoD SIAO and DISN DAAs for information system connections to the DISN. It is the DISN community forum for reviewing and resolving C&A decisions related to sharing of community risk.

E2.1.18. Denial of Authorization to Operate (DATO). DAA determination that a DoD information system cannot operate because of an inadequate IA design, failure to adequately implement assigned IA Controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

E2.1.19. Designated Accrediting Authority (DAA). Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approving Authority and Delegated Accrediting Authority.

E2.1.20. DIACAP Implementation Plan. The Implementation Plan contains the information system's assigned IA Controls. The plan also includes the implementation status, responsible entities, resources and the estimated completion date for each assigned IA Control. The plan may reference applicable supporting implementation material and artifacts.

E2.1.21. DIACAP Knowledge Service. A web-based repository of information and tools for implementing the DIACAP that is maintained through the DIACAP TAG.

E2.1.22 DIACAP Package. The collection of documents or collection of data objects generated through DIACAP implementation for an information system. A DIACAP package is developed through implementing the activities of the DIACAP and maintained throughout a system's life cycle. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. There are two types of DIACAP package, the Comprehensive Package containing all information connected with the certification of the information system, and the Executive Package containing minimum information for an accreditation decision. The Comprehensive package contains the System Identification Profile (SIP), the DIACAP Implementation Plan, the Certification Documentation, the DIACAP Scorecard, and the POA&M if required. The Executive package contains the System Identification Profile,

Untitled

the DIACAP Scorecard, and the POA&M if required.

E2.1.23. DIACAP Scorecard. A summary report that shows the certified or accredited implementation status of a DoD information system's assigned IA Controls and supports or conveys a certification determination and/or accreditation decision. The DIACAP Scorecard is intended to convey information about the IA posture of a DoD information system in a format that can be easily understood by managers and be easily exchanged electronically.

E2.1.24. DIACAP Team. The officials responsible for implementing the DIACAP for a DoD information system. At a minimum the DIACAP Team includes the DAA, the CA, the SIAO, the DoD information system PM or SM, the DoD information system IAM, IA0, and a User Representative.

E2.1.25. DoD Information Assurance Certification and Accreditation Process (DIACAP). The DoD processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, Federal and DoD requirements.

E2.1.26. DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections. DoDD 8500.1 (reference (b)).

E2.1.26.1. Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in DoD Directive 5000.1 (reference (i)). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support (ICIS)); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System (GCCS), Defense Messaging System (DMS)). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note: an AIS application is analogous to a "major application" as defined in OMB A-130 (reference (n)); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS).

E2.1.26.2. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single approval authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130 (reference (n)). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

E2.1.26.3. Outsourced IT-based process. For DoD information assurance purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Untitled

E2.1.26.4. Platform IT Interconnection. For DoD information assurance purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Examples of platform IT interconnections that impose security considerations include remote administration and remote upgrade or reconfiguration. Also see Platform IT.

E2.1.27. Enclave. See DoD Information System.

E2.1.28. Enterprise Information Environment (EIE). The common, integrated computing and communications environment of the Global Information Grid (GIG). The GIG EIE is composed of assets that operate as or that assure local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks, and wide area networks. The GIG EIE is also composed of assets that operate as or in direct support of end user devices, workstations, and servers that provide local, organizational, regional, or global computing capabilities. The GIG EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The GIG EIE includes a common set of Enterprise and mission specific services, called GIG Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG. DoDI 8115.01 (reference (h)).

E2.1.29. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (o)). The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. DoDD 8100.1 (reference (c)).

E2.1.29.1. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.29.1.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.29.1.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.29.1.3. Processes data or information for use by other equipment, software, or services.

E2.1.29.2. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

E2.1.30. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. DoDD 8500.1 (reference (b)).

E2.1.31. Inheritance. Inheritance in the context of DIACAP refers to the state in which an IA Control along with the control's validation results and compliance status, is shared across two or more systems for the purposes of C&A. Through inheritance, an existing IA Control and its C&A status, would extend from an

Untitled

"originating" system to another "receiving" system in order to model a real-world scenario of shared security infrastructure or capability. Inheritance is intended to reduce the complexity of testing by allowing the unilateral application of validation test results to all systems sharing the security capability. The DIACAP Implementation Plan specifically identifies IA Controls inherited between systems.

E2.1.32. IA Capabilities and Services. Information technology (hardware, software, and firmware), data, facilities, and human activities designed and implemented to provide integrity, confidentiality, non-repudiation, identification and authentication, and availability of DoD information systems through the exercise of management, operational, technical, and personnel controls.

E2.1.33. IA Component of the GIG. The collective and interdependent IA capabilities and services of the information systems that comprise the GIG.

E2.1.34. IA Component of the GIG Architecture. An abstract expression of current and future instances of the IA Component of the GIG.

E2.1.35. IA Component of the System Architecture. An abstract expression of all current or future IA/security technical solutions employed within a DoD information system and all interfaces to core enterprise or COI services for IA/security. The IA/security architecture assigns and portrays the assigned IA roles and behavior of all inherent IA/security features and functions and all embedded IA or IA-enabled IT products, and prescribes rules for interaction and interconnection. The IA component of the system architecture must conform to the IA Component of the GIG Architecture.

E2.1.36. IA Control. An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with DoDI 8500.2.

E2.1.37. IA Control Set. Collection of IA Controls associated with a level of integrity, availability, and confidentiality.

E2.1.38. Information Assurance Manager (IAM). The individual responsible for the information assurance program of a DoD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the title Information Systems Security Manager (ISSM). DoDI 8500.2.

E2.1.39. Information Assurance Officer (IAO). An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. DoDI 8500.2.

E2.1.40. Information Assurance Senior Leadership Group (IASL). This senior leadership group provides strategic direction and guidance to ensure integrated Defense-wide IA. It provides for the integrated planning, coordination, and oversight of the Department's IA programs. In addition, the group will establish the relationships required to ensure IA is designed into the Global Information Grid (GIG) integrated architectures.

E2.1.41. Information Assurance Support Environment (IASE). A web based resource providing access to current DoD and Federal IA and IA-related policy and guidance, including recent and pending legislation. DoDI 8500.2.

E2.1.42. Impact Code. Indicates DoD's assessment of the likelihood that a failed IA control will have IA consequences that have system-wide consequences. It is an indicator of the impact associated with non-compliance or exploitation of the IA Control. May also indicate the urgency with which corrective action should be taken. Impact codes are expressed as High, Medium, Low where High is the indicator of greatest impact or urgency.

## Untitled

E2.1.42.1. High Impact Code. The absence or incorrect implementation of this IA Control may result in the loss of information resources, unauthorized disclosure of information, or failure to maintain information integrity. Such exploitation may severely disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

E2.1.42.2. Medium Impact Code. The absence or incorrect implementation of this IA Control may moderately disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

E2.1.42.3. Low Impact Code. The absence or incorrect implementation of this IA Control may minimally disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

E2.1.43. Implementation Procedures. Describes the required steps and provides guidance for implementing DoD IA Controls.

E2.1.44. Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

E2.1.45. Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology. DoDD 8000.1

E2.1.46. Information System (IS). Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display or transmission of information. CNSSI No. 4009.

E2.1.47. Information Systems Security Engineering/Engineer (ISSE). An engineering process or individual that captures and refines information protection requirements and ensures their integration into IT acquisition processes through purposeful security design or configuration.

E2.1.48. Interim Authorization to Operate (IATO). Temporary authorization to operate a DoD information system under the conditions or constraints enumerated in the accreditation decision.

E2.1.49. Interim Authorization to Test (IATT). Temporary authorization to test a DoD information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the accreditation decision.

E2.1.50. Mission Area (MA). A defined area of responsibility whose functions and processes contribute to accomplishment of the mission. Those mission areas are: The War Fighting Mission Area (WMA), Business Mission Area, (BMA), DoD portion of the Intelligence Mission Area (DI MA), and Enterprise Information Environment Mission Area (EIE MA).

E2.1.51. Mission Assurance Category (MAC). Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories.

E2.1.51.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

## Untitled

E2.1.51.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.

E2.1.51.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

E2.1.52. Net-centricity. Net-centricity is a robust, globally connected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-centric capabilities enable network-centric operations and Net-Centric Warfare (NCW) DoDD 8320.2.

E2.1.53. Outsourced IT-based Process. See DoD Information System.

E2.1.54. Platform IT. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric.

E2.1.55. Platform IT Interconnection. See DoD Information System.

E2.1.56. Plan of Action and Milestones (POA&M). A plan of action and milestones is required for any accreditation decision that requires corrective actions. It is a tool identifying tasks that need to be accomplished. It specifies resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

E2.1.57. Principal Accrediting Authority (PAA). The senior official having the authority and responsibility for information systems within a GIG Mission Area.

E2.1.58. Program or System Manager (PM or SM). Official responsible for the early and seamless integration of information assurance into and throughout the system life cycle of an assigned DoD information system.

E2.1.59. Proxy. Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

E2.1.60. Residual Risk. Risk due to partial or unsatisfactory implementation of assigned IA Controls.

E2.1.61. Risk Management. Achieving and maintaining an acceptable IA posture (i.e., adequate security, interoperability, and visibility within IA situational awareness or command and control systems) through the implementation of assigned IA Controls. IA Controls are assigned based on the value of the information being processed and

the extent of information environment being shared.

E2.1.62. Security Relevant Event. An event that would cause a harmful change in an information system or its environment, or that a competent IAM would consider to require noting, investigation, or prevention (e.g., the discovery of malicious code in an information system, the discovery of an attempt to connect an unapproved device to the network).

E2.1.63. Senior Information Assurance Officer (SIAO). Official responsible for directing an organization's information assurance program on behalf of the organization's CIO.

E2.1.64. Service. A unit of work or specific operation done by a service provider to achieve a desired end result for a service consumer.

E2.1.65. Service Oriented Architecture (SOA). An architectural style whose goal is to achieve loose coupling or minimal dependency among interacting proxies through a small set of simple and ubiquitous interfaces among all participating proxies and descriptive messages constrained by an extensible schema delivered through the interfaces. Also, a specific type of system in which each proxy is called a "service" because it performs some well-defined operation (i.e., "provides a service") that can be invoked outside of the context of a larger application. That is, a service might be implemented to expose a feature of a larger application (e.g., the purchase order processing capability of an enterprise resource planning system might be exposed as a discrete service), and the users of that service need be concerned only with the interface description of the service. Security requirements for interaction are addressed in design and in the interface description, thus allowing proxies to dynamically interact with services outside the accreditation boundary.

E2.1.66. Severity Code. Indicates the CA's assessment of the likelihood of system-wide IA consequences, given a single or multiple findings. It is the Code assigned to a system IA security weakness by a CA as part of a certification analysis to indicate (1) the risk level associated with the IA security weakness and (2) the urgency with which the corrective action must be completed. Severity codes are expressed as "CAT I, CAT II, CAT III," where CAT I is the indicator of greatest risk and urgency.

E2.1.66.1. CAT I Severity Code. Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges, and usually cannot be mitigated.

E2.1.66.2. CAT II Severity Code. Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT II findings can usually be mitigated and will not prevent an ATO from being granted.

E2.1.66.3. CAT III Severity Code. Assigned to recommendations that will improve IA posture but are not required for an authorization to operate.

E2.1.67. Stand-Alone Information System. An information system operating independently of any other information system within an environment physically secured commensurate with the highest classification of material processed or stored thereon. DoDI 8580.1 (reference (t)).

E2.1.68. System Identification Profile (SIP). An information base, i.e., a document, collection of documents, or collection of data objects within an automated information system, that uniquely identifies an information system within the DIACAP and contains established management indicators, e.g., DIACAP status.

E2.1.69. User Representative (UR). Individual or organization that represents the user community in the DIACAP.

E2.1.70. Validation. Activity applied throughout the system life cycle, to confirm

## Untitled

or establish by testing, evaluation, examination, investigation, or competent evidence that a DoD information system's assigned IA Controls are implemented correctly and are effective in their application.

E2.1.71. Validation Event. The execution of one or more Validation Procedures for a DoD information system.

E2.1.72. Validation Procedure. Describes the requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results, and may include associated supporting background material, sample results, or links to automated testing tools.

E2.1.73. Validator. Entity responsible for conducting a validation procedure.

E2.1.74. Web Services. Self-describing, self-contained, modular units of software application logic that provide defined business functionality. Web services are consumable software services that typically include some combination of business logic and data. Web services can be aggregated to establish a larger workflow or business transaction. Inherently, the architectural components of web services support messaging, service descriptions, registries, and loosely coupled interoperability.

## ACRONYMS

ACAT Acquisition Category  
ACTD Advanced Concept Technology Demonstration  
ASD(NII) Assistant Secretary of Defense for Networks and Information Integration  
AIS Automated Information System  
ATD Authorization Termination Date  
ATO Authorization to Operate  
BMA Business Mission Area  
C&A Certification and Accreditation  
CA Certifying Authority  
CCA Clinger Cohen Act  
CCM Configuration Control and Management  
CDS Cross Domain Solution  
CES Core Enterprise Services  
CFO Chief Financial Officer  
CIO Chief Information Officer  
CJCS Chairman Joint Chiefs of Staff  
CJCSI CJCS Instruction  
CL Confidentiality Level  
C/NC Compliant/Non-compliant  
CNDSP Computer Network Defense Service Provider  
CNSS Committee on National Security Systems  
CNSSI Committee on National Security Systems Instruction  
COI Communities of Interest  
COTS Commercially Owned Technology Services  
DAA Designated Accrediting Authority  
DATO Denial of Authorization to Operate  
DCID Director Central Intelligence Directive  
DIACAP DoD Information Assurance Certification and Accreditation Process  
DICAST Defense and Intelligence Community Accreditation Support Team  
DIMA Defense Intelligence Mission Area  
DISA Defense Information Systems Agency  
DISN Defense Information Systems Network  
DITSCAP DoD Information Technology Security Certification and Accreditation Process  
  
DITPR Defense Information Technology Portfolio Repository  
DMS Defense Messaging System  
DNI Director of National Intelligence

Untitled

DoD Department of Defense  
DoDD DoD Directive  
DoDI DoD Instruction  
DOT&E Director, Operational Test and Evaluation  
DSAWG Defense IA/Security Accreditation Working Group (formerly DISN Security Accreditation Working Group)  
EIE Enterprise Information Environment  
EIEMA Enterprise Information Environment Mission Area  
FISMA Federal Information Security Management Act  
GAO Government Accountability Office  
GCCS Global Command and Control System  
GIG Global Information Grid  
GOGO Government Owned Government Operated  
GOTS Government Owned Technology Services  
IA Information Assurance  
IAM Information Assurance Manager  
IAO Information Assurance Officer  
IASE Information Assurance Support Environment  
IASL Information Assurance Senior Leadership Group  
IATO Interim Authorization to Operate  
IATT Interim Authorization to Test  
IC Intelligence Community  
ICIS Integrated Consumable Item Support  
ID Identification  
IG Inspector General  
ISSE Information Systems Security Engineer/Engineering  
ISSM Information Systems Security Manager  
IT Information Technology  
JCIDS Joint Capabilities Identification and Development System  
KS Knowledge Service  
MA Mission Area  
MAC Mission Assurance Category  
MAIS Major Automated Information System  
MC Mission Critical  
ME Mission Essential  
MS Mission Support  
MS-A, B or C [Acquisition] Milestone A, B, or C  
NCOW-RM Net-Centric Operations and Warfare Reference Model  
NIPRNet Non-Classified Internet Protocol Router Network  
NSA National Security Agency  
NSS National Security Systems  
NSTISSP National Security Telecommunications and Information Security Policy  
OMB Office of Management and Budget  
OSD Office of the Secretary of Defense  
PAA Principal Accrediting Authority  
PM or SM Program or System Manager  
POA&M Plan of Action and Milestones  
POC Point of Contact  
PPBE Planning, Programming, Budgeting and Execution  
PPSM Ports, Protocols and Services Management  
RTM Requirements Traceability Matrix  
SAP Special Access Program  
SAR Special Access Requirement  
SCI Sensitive Compartmented Information  
SEP System Engineering Plan  
SIAO Senior Information Assurance Officer  
SIP System Identification Profile  
SIPRNet Secret Internet Protocol Router Network  
SLC System Life Cycle  
SOA Service Oriented Architecture  
SSAA System Security Authorization Agreement  
TAG Technical Advisory Group  
TEMP Test and Evaluation Master Plan

Untitled

UR User Representative

USD(AT&L) Under Secretary of Defense for Acquisition, Technology and Logistics

USI Universal System Identifier

WMA Warfighting Mission Area