APPENDIX K - GLOSSARY

Term	Definition
Authorization decision	A formal statement by an Authorizing Official regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim authorization to test (IATT), or denial of ATO (DATO). The Authorization decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD public key infrastructure (PKI)-certified digital signature. (ref j)
Approval to Connect (ATC)	A formal statement by the Connection Approval Office granting approval for an IS to connect to the DISN. The ATC cannot be granted for longer than the period of validity of the associated ATO. An ATO may be issued for up to 3 years.
Artifacts	System policies, documentation, plans, test procedures, test results, and other evidence that express or enforce the cybersecurity posture of the DoD IS, make up the Assessment and Authorization (A&A) documentation (for RMF packages) or Certification & Accreditation (C&A) information (for DIACAP package), and provide evidence of compliance with the assigned cybersecurity controls. (ref d)
Authorization to Operate (ATO)	Authorization granted by a DAA/AO for a DoD IS to process, store, or transmit information; an ATO indicates a DoD IS has adequately implemented all assigned cybersecurity controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to three (3) years. (ref j)
Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (ref j) ("Authorizing Official is the RMF term that supersedes the term "Designated Accrediting Authority" used under DIACAP)
Authorization Termination Date (ATD)	The date assigned by the DAA/AO that indicates when an ATO or IATT expires.
Connection Approval Process (CAP)	Packages provide the CAO the information necessary to make the connection approval decision.
Certification	A comprehensive evaluation and validation of a DoD IS to establish the degree to which it complies with assigned cybersecurity controls based on standardized procedures. (ref j) (Note: this term is superseded by "Assessment.")
Certification Determination	A CA's determination of the degree to which a system complies with assigned cybersecurity controls based on validation results. It identifies and assesses the residual risk with operating a system and the costs to correct or mitigate cybersecurity security weaknesses as

	documented in the Information Technology (IT) Security Plan of Action and Milestones (POA&M)
Certifying Authority (CA)	The senior official having the authority and responsibility for the certification of Information Systems governed by a DoD Component cybersecurity program.
Consent to Monitor (CTM)	This is the agreement signed by the DAA/AO granting DISA permission to periodically monitor the connection and assess the level of compliance with cybersecurity policy and guidelines.
Connection Approval Process	Formal process for adjudication requests to interconnect information systems.
Connection Approval Office (CAO)	Single point of contact within DISA for all DISN connection approval requests.
Command Communications Service Designator (CCSD)	A unique identifier for each single service including use circuits, package system circuits, and interswitch trunk circuits.
Computer Network Defense (CND)	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.
Cybersecurity Service Provider	DoDI 8530.01 (ref k) requires DoD IT to be aligned to a DoD network operations and security centers (NOSCs). The NOSC and supporting cybersecurity service provider(s) will provide any required cybersecurity services to aligned systems. Cybersecurity Service Providers will: (1) Offer and provide cybersecurity services in accordance with DoD O-8530.01-M (ref L). (2) Execute cybersecurity responsibilities and authorities in accordance with DoD Component policy, MOAs, contracts, or support agreements. (3) Comply with directives and orders of USSTRATCOM and supported DoD Component NOSC and organizations. (4) Document all supported entities and associated systems in accordance with DoD Component policy, MOAs, contracts, or support agreements.
Cross Domain Appendix (CDA)	In support of the A&A of a CDS, this appendix defines the security requirements, technical solution, testing, and compliance information applicable to the cross-domain connection.
Cross Domain Solution (CDS)	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. (ref ad)
Customer	There are two general types of DISN customers/partners: DoD and non-DoD customers. DoD customers are DoD Combatant Commands, Military Services and Organizations, and Agencies (DoD CC/S/A/), collectively referred to as "DoD Components." Non-DoD customer include includes: contractors and federally funded research and development centers, other U.S. government federal departments and agencies, state, local, and tribal governments, foreign government organizations/entities (e.g., allies or coalition partners), non-government organizations, commercial companies and industry,

	academia (e.g., universities, colleges, or research and development centers), etc. and are collectively referred to as "Mission Partners."
Defense Information Systems Connection Process Guide (DISN CPG)	Step-by-step guide to the detailed procedures that Customers must follow in order to obtain and retain connections to the DISN (ref am).
Defense Information Systems Network (DISN)	DoD integrated network, centrally managed and configured to provide long-haul information transfer for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery and video teleconferencing services.
Defense Information Systems Network-Leading Edge Services (DISN-LES)	Defense Information Systems Network-Leading Edge Services (DISN-LES) is a Mission Assurance Category III program designed to pass encrypted unclassified and classified traffic over the Classified Provider Edge (CPE) routers of the DISN, and provide capability for subscriber sites requiring "next generation" network, encryption, software, NETOPS, and advanced services not offered by other DISN Subscription Services (DSS). The network provides a non-command-and-control, risk aware infrastructure identical to the core DISN data services (NIPRNet and SIPRNet).
Denial of Approval to Connect (DATC)	A formal statement by the Connection Approval Office withholding (in the case of a new connection request) or rescinding (in the case of an existing connection) approval for an IS to connect (or remain connected) to the DISN.
Denial of Authorization to Operate (DATO)	A DAA/AO decision that a DoD IS cannot operate because of an inadequate cybersecurity design, failure to adequately implement assigned cybersecurity controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.
Department of Defense Information Network	The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security."
Designated Accrediting Authority (DAA)	The 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. (Superseded by the RMF term "Authorizing Official)
DISA Defense Enterprise Computing Center (DECC)	Services provided within a backdrop of world-class computing facilities located in both the continental United States (CONUS) and outside of the continental United States (OCONUS).
Defense Information Assurance Certification and	The DoD processes for identifying, implementing, validating, certifying, and managing cybersecurity capabilities and services, expressed as cybersecurity Controls, and authorizing the operation of

Accreditation Process (DIACAP)	DoD information systems in accordance with statutory, Federal and DoD requirements. (The Risk Management Framework (RMF) supersedes DIACAP as stipulated in DoDI 8510,01 (ref d))
Defense Security/Cybersecurity Authorization Working Group (DSAWG)	Provides, interprets, and approves DISN security policy, guides architecture development, and recommends Authorization decisions to the DISN Flag panel. Also reviews and approves Cross Domain information transfers (as delegated from the DISN/DODIN Flag Panel) or forwards such recommendation(s) to the Flag Panel.
DIACAP Scorecard	A summary report that succinctly conveys information on the cybersecurity posture of a DoD IS in a format that can be exchanged electronically; it shows the implementation status of a DoD Information System's assigned cybersecurity controls (i.e., compliant (C), non-compliant (NC), or not applicable (NA)) as well as the C&A status. (DIACAP is superseded by DoDI 8510.01 (ref d))
Demilitarized Zone (DMZ)	Physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
Defense Information Systems Agency (DISA) Direct Order Entry (DDOE)	This is the ordering tool for DISN telecommunications services.
DoD Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. It includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections. (ref c)
DoD Component	DoD Combatant Commands, Military Services and Organizations, Agencies, and Field Activities (CC/S/A), which are collectively referred to as DoD Components.
DoD Unified Capabilities (UC) Approved Products List (APL)	Is established in response to DoDI 8100.04 DoD Unified Capabilities (UC) and the Unified Capabilities Requirements (UCR Change III September 2011). Its purpose is to provide Interoperability (IO) and cybersecurity authorized products for DoD Components to acquire and to assist them in gaining approval to connect to DoD networks in accordance with policy.
DODIN Readiness and Security Inspections (DRSI)	Produces and deploys cybersecurity products, services, and capabilities to combatant commands, services, and agencies to protect and defend the Global Information Grid (GIG).
DODIN Interconnection Approval Process (GIAP)	Electronic process to submit connection information and register a DODIN connection.
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. (ref o)
IA Certification and Accreditation	The legacy DoD approach (under DIACAP) for identifying information security requirements, providing security solutions and managing the security of DoD information systems. (ref o) (Superseded by Assessment/Authorization)
Information Systems (IS)	Computer-based information systems are complementary networks of hardware/software that people and organizations use to collect, filter, process, create, and distribute data.
Interim Approval to Connect (IATC)	Temporary approval granted by the Connection Approval Office for the connection of an IS to the DISN under the conditions or constraints enumerated in the connection approval. An IATC is normally granted for no more than 180 days. IATCs may be granted for up to one year for units deployed in the CENTCOM AOR.
Interim Authorization to Test (IATT)	A temporary authorization to test a DoD IS in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the Authorization decision.
Interim Certificate to Operate (ICTO)	Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO will be made by the MCEB Interoperability Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.
Internet Protocol (IP)	Protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.
Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (ref o)
Mission Partner	Those with whom Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments, allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. (DoDD 8000.01)
Plan of Action & Milestones (POA&M)	A permanent record that identifies tasks to be accomplished in order to resolve security weaknesses; required for any Authorization decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks; also used to document DAA-accepted non-compliant cybersecurity controls and baseline cybersecurity controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.
Platform Information Technology (PIT)	Defined in ref a

Program or System Manager (PM or SM)	The individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs.
Request For Service (RFS)	The document, used to initially request telecommunications service, which is submitted by the requester of the service to his designated TCO.
Risk Management Framework	A structured approach used to oversee and manage risk for an enterprise. (ref j))
Service Delivery Point (SDP)	The point at which a user connects to the DISN. The DISN provides cybersecurity controls up to the SDP. The Partner/user is responsible for cybersecurity controls outside of the SDP.
System Identification Profile (SIP)	A compiled list of system characteristics or qualities required to register an IS with the governing DoD Component cybersecurity program.
Telecommunications Certification Office (TCO)	The activity designated by a Federal department or agency to certify to DISA (as an operating agency of the National Communications System) that a specified telecommunications service or facility is a validated, coordinated, and approved requirement of the department or agency, and that the department or agency is prepared to pay mutually acceptable costs involved in the fulfillment of the requirement.
Telecommunications Service Order (TSO)	The authorization from Headquarters, DISA, a DISA area, or DISA-DSC to start, change, or discontinue circuits or trunks and to effect administrative changes.
Telecommunications Service Request (TSR)	Telecommunications requirement prepared in accordance with chapter 3, DISAC 310-130-1 and submitted to DISA or DISA activities for fulfillment. A TSR may not be issued except by a specifically authorized TCO.
Unified Capabilities (UC)	The seamless integration of voice, video, and data applications services delivered ubiquitously across a secure and highly available Internet Protocol (IP) infrastructure to provide increased mission effectiveness to the warfighter and business communities. UC integrate standards-based communication and collaboration services including, but not limited to, the following: messaging; voice, video and Web conferencing; Presence; and UC clients. (ref g)
Unified Cross Domain Services Management Office (UCDSMO)	The UCDSMO provides centralized coordination and oversight of all cross-domain initiatives across the Department of Defense and the Intelligence Community.
Virtual Private LAN (VPL)	Means to provide Ethernet-based multipoint-to-multipoint communication over IP/MPLS networks.
Wide Area Network (WAN)	A computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries).