Department of Defense (DoD) Information Enterprise Architecture

Mission Partner Environment LEXICON

Version 1.0

August 12, 2016

Prepared by:
Director, Architecture & Engineering
Office of the DoD Chief Information Officer (CIO)

DISTRIBUTION STATEMENT A. Approved for public release

[This page intentionally left blank]

SIGNATURE PAGE

Submitted By:

LAM.NGOAN.THOMAS.1229438960

Digitally signed by LAM.NGOAN.THOMAS.1229438960
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OSD, cn=LAM.NGOAN.THOMAS.1229438960
Date: 2016.08.10 13:41:02 -04'00'

MR. TOM LAM, GS-15
Chief Architect
Mission Partner Environment – Information System (MPE-IS)
Deputy Director of Architecture & Engineering
Office of the Department of Defense Chief Information Officer (DoD CIO)

Approved By:

KINNEY.RORY.S.1130078733

Digitally signed by KINNEY.RORY.S.1130078733
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OSD, cn=KINNEY.RORY.S.1130078733
Date: 2016.08.25 15:58:24 -04'00'

MR. RORY KINNEY, SES
Project Lead
Mission Partner Environment – Information System (MPE-IS)
Director of Architecture and Engineering
Office of the Department of Defense Chief Information Officer (DoD CIO)

DOCUMENT HISTORY

Version	Date	POC	Brief Description
0.1	16 JUL 15	Tom Lam	Initial MS Word formatted draft
0.2	27 JUL 15	Tom Lam	Redesigned document into 4 Sections, updated definitions and streamlined the presentation of Term, Definitions, Types, and Acronyms; included comments from 5 sources.
0.3	31 AUG 15	Tom Lam	Incorporated comments from DoD CIO CS, NGB, CENTCOM, PACOM, NSA, DISA JTSO, MNIS Office, BICES Office, CIAV, and DISA JITC. Plus corrected additional minor formatting errors in document. The Lexicon was expanded to include more system descriptions. 3 Appendices were added to better identify the Systems and Services, and to list all the acronyms in one location. Prepared the document for formal coordination.
0.4	11 DEC 15	Tom Lam	Incorporated first round of formal review inputs
0.5	14 MAR 16	Tom Lam	Incorporates comments from the C/S/A coordination. Restructures the Lexicon and scales it back by removing general IT and DoD terms that are not important to MPE.
0.90	7 APR 16	Tom Lam	Incorporates feedback from the final stakeholder review.
1.0	12 AUG 16	Tom Lam	Initial release.

TABLE OF CONTENTS

APPENDICES

1 Introduction

Information sharing with mission partners is enabled through a complex web of doctrine, training, and policy enabled by programs, systems, and technologies involving hundreds of organizations and many thousands of individuals. Given this complexity and the importance of effective communications to mission success, a consistent, repeatable vocabulary is necessary to minimize miscommunication, misinterpretation, or confusion about the meaning of commonly used terms and phrases. This lexicon is intended to help establish a controlled vocabulary for the use of Mission Partner Environment (MPE) and MPE-related terms across the Department and with our varied mission partners.

1.1 Purpose and Intended Use

The MPE Lexicon is intended for all operators, maintainers, developers, and other stakeholders (including mission partners) of the United States (U.S.) Department of Defense (DoD) portion of the global MPE. It is a mechanism for clearly and consistently communicating the desired intent and effect of the mission/ event/exercise commander. The terms and their associated definitions found in the lexicon will be used in all documents and other media related to the DoD portion of the MPE to the greatest extent possible. Unless otherwise stated, the terms and definitions contained in this Lexicon are for the MPE community only. The same terms may have different meanings for other communities.

1.2 Initial Development

The initial set of Lexicon terms and definitions was collected from multiple DoD and industry sources and shaped through a collaborative process involving various DoD components. The Lexicon was scoped to narrowly focus on terms that have a specific meaning within the context of MPE (but may have a different meaning in a different context) and terms that are sometimes misused or confused.

1.3 Maintaining and Updating the Lexicon

A one-time, static lexicon will not serve the MPE community as new terms will need to be added and existing terms will need to be modified on a regular basis. For this reason, the DoD Chief Information Officer (CIO) will manage the Lexicon through a Public Key Infrastructure-enabled wiki site. Any member of the MPE community with appropriate credentials will be able to go into the site and use simple wiki edit techniques to suggest additions, deletions, or modifications. The DoD CIO will review and finalize proposed changes on a regular basis. The MPE Lexicon site URL is:

https://www.milsuite.mil/wiki/MPE_Lexicon

1.4 Use of Sources

Every attempt was made to define terms based on recognized, official sources with an established pedigree. Sources were chosen based on a number of criteria including applicability to the MPE space, confidence level (as those levels are defined in the Joint Staff J6 AV-2 Development Guide), and date (more recent sources were preferred over older sources). In some cases, a definition was derived from a source (or sources) rather than defined exactly as the source defined it. This was necessary for elements that needed to be defined in the context of MPE or for elements where no exact match was found within the authoritative sources. In those cases, the source is appended with, “(Derived from:)”. Following, is the hierarchy of sources used in this Lexicon:

1) U.S. national security sources (e.g., Committee On National Security Systems)
2) Office of the Secretary of Defense (OSD) and Joint Staff sources (e.g., policy issuances, joint publications)
3) Combatant Commands/Military Services/Defense Agencies (CC/S/A) sources (e.g., architectures, concepts of operations)

4) U.S. Federal sources (e.g., National Institute of Standards and Technology)
5) Industry sources (used as the basis for terms that are widely used in industry)
6) Mission Partner Environment-Information System (MPE-IS) Senior Engineering Work Group (WG) or WG documents

1.5 Lexicon Format

Each entry follows the format shown below:

Term (Acronym) – Identifies the word or phrase of interest and its commonly used acronym, if one exists.

Definition – A brief definition of the word or phrase taken from or derived from the listed source(s). Where appropriate the definition is stated in an MPE context rather than a more generalized definition that may have a different meaning outside of MPE.

Source – The authoritative document(s) from which the definition was taken or derived. Use of the phrase "Derived from" indicates the definition is not an exact word-for-word rendering from a source, but that the source(s) was used as the primary basis for creating the given definition.

See Also – Optional field used to indicate other entries in the Lexicon that are related to the subject entry.

Reference – Optional field used to provide additional information on the subject entry such a website.

Acknowledgement

The DoD CIO would like to thank the DoD MPE community for their help in developing this lexicon; no project of this magnitude and importance could have been accomplished by only one organization. The ongoing usefulness of the lexicon will depend upon the willingness of the community to collaboratively update it as the MPE vocabulary evolves over time.

2 Lexicon

2.1 A-Terms

Afghanistan Mission Network (AMN)

Definition

The primary Coalition Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C5ISR) network in Afghanistan for all International Security Assistance Force (ISAF) forces and operations. It is a federation of networks with the AMN Core provided by North Atlantic Treaty Organization (NATO) and national network extensions provided by contributing nations. The AMN is operated as a single security domain in order to facilitate information sharing between participating nations without security boundaries.

Source
Future Mission Network 90-day Study Report, 17 December 2012

Agile Virtual Enclave (AVE)

Definition
A Virtual Private Network (VPN) formed using Internet Protocol Security (IPSec) and additional security measures to form the different network security information sharing and data exchange domains across a common "black core" transport. These virtual enclaves are subject to quality of service allowing information packets to be prioritized and routed in accordance with the policy, precedence, and operational control. Agile Virtual Enclaves can be created and removed quickly, enabling information sharing and data exchange with unanticipated mission partners and reuse of the full network capability. The preferred general term is Mission Enclave, and the use of the term AVE is typically used in conjunction with Multi-Enclave Clients.

Source
U.S. DoD Episodic Mission Partner Environment Joining Instructions, Version 1.10, 11 August 2014

See Also
Mission Partner Environment – Information System (MPE-IS) Mission Enclave
Multi-Enclave Client (MEC)

Alliance

Definition
The relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members.

Source
Joint Publication (JP) 3-0, 11 August 2011

See Also
Coalition

All Partners Access Network (APAN)

Definition
A web collaboration platform which enables UNCLASSIFIED information exchange between the U.S. DoD and international partners, organizations, agencies, or individuals who do not have access to traditional DoD communication systems. APAN provides a set of shared enterprise Web 2.0 services

managed by the Defense Information Systems Agency (DISA) that combines the benefits of unstructured collaboration (wikis, blogs, forums) and structured collaboration (file sharing, calendar) with the personalization of social networking.

Source
Derived from: Multi-National Information Sharing Program Office overview found on www.disa.mil

Reference
APAN Website, www.apan.org

Application Service Points (ASP)

Definition
A set of servers that support users of a mission enclave with specified application services (e.g., Web, Email, Voice over Internet Protocol (VoIP), Chat).

Source
Derived from: DoD Cybersecurity Reference Architecture (CS RA) Version 3.0 (FINAL), 24 September 2014 and the Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

Asia-Pacific Intelligence Information Network (APIIN)

Definition
USBICES-X/ Asia-Pacific Intelligence Information Network (APIIN) supports intelligence sharing and intelligence support to operations through bi-lateral and potentially multi-lateral networks. The network services include email, VOIP, HD-VTC, and file sharing. The APIIN networks may be connected to the Trusted Network Environment (TNE®) enabling cross domain email and file sharing within agreed upon sharing arrangements.

Source
Derived from: USPACOM documentation

2.2 B-Terms

Battlefield Information Collection and Exploitation Systems (BICES)

Definition
An intelligence system that allows intelligence data/information sharing among 28 North Atlantic Treaty Organization (NATO) nations, 7 non-NATO nations; shares information/intelligence in peace and crisis, in bi-lateral and multi-lateral environments; and with national military intelligence organizations. The BICES Backbone Network (BBN) is funded by the nations. Each nation connects to the BBN for connectivity to the other NATO nations as well as NATO's SECRET Wide Area Network (NS WAN) and Headquarters (HQ) NATO's Minerva network. Connectivity with BICES allows secure Web and Email with over 65,000 NATO and national users and Secure Voice or Video with over 700 users worldwide. BICES operates at the NATO SECRET classification level. BICES maintains Cross Domain Solutions (CDS) that enable data to be passed to seven participating non-NATO nations, including Australia, Austria, Finland, Ireland, New Zealand, Sweden, and Switzerland.

Source
U.S. Battlefield Information Collection and Exploitation Systems (BICES) Service Catalog v3.0, Battlefield Information Collection and Exploitation Systems (BICES) 2014 Service Catalogue

See Also
U.S. Battlefield Information Collection and Exploitation Systems
U.S. Battlefield Information Collection and Exploitation Systems - Extended

Black Core

Definition
A communication network architecture in which user data traversing a global Internet Protocol (IP) network is end-to-end encrypted at the IP layer. Related to striped core.

Source
Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015

Black Transport

Definition
A network environment (point-to-point and multi-point) supporting end-to-end encrypted information at a single classification level; networks within the environment are segmented by network technology with inspection points at the perimeter, boundary, or gateway. Encrypted traffic is routed, switched, or forwarded over an UNCLASSIFIED or untrusted network infrastructure, which may or may not be controlled by the DoD.

Source
Joint Information Environment (JIE) Network Normalization and Transport (NNT) Integrated Design Team (IDT) Wide Area Network (WAN) Solution Architecture

2.3 C-Terms

Capabilities/Limitations, Operational Impacts (CAPs/LIMs, OIs)

Definition
Capabilities (CAPs) - The ability of a mission thread (MT) service to support the minimum operational requirement (MOR) for the MT during execution of an operational mission.
Limitations (LIMs) - The areas in which an MT service fails to support the MOR and Minimum Implementation (MINIMP) for MTs in the execution of an operational mission.
Operational Impacts (OI) - The effect upon the operational commander’s ability to conduct his mission resulting from the identified capabilities and limitations identified from the analysis of the MOR and MINIMP.

Source
Coalition Interoperability Assurance and Validation (CIAV) Mission Profiles Implementation Strategy

CENTCOM Partner Network (CPN)

Definition
A “network of networks” utilizing U.S. and coalition networks to establish an enduring regional partner network for command and control (C2), secure communication, information sharing, and coordination between USCENTCOM, our service components and assigned JTF’s and regional partners operating at the strategic/operational level.

Source
USCENTCOM Update to Coalition Capability Exchange Meeting (CCEM), 3 December 2014

Coalition

Definition
A coalition is an arrangement between two or more nations for common action. Coalitions are typically ad hoc, formed by different nations, often with different objectives, usually for a single event or for a longer period while addressing a narrow sector of common interest. Operations conducted with units from two or more coalition members are referred to as coalition operations.

Source
Derived from: Joint Publication 1-02, 15 June 2015 and Joint Publication 3-16

Coalition Interoperability Assurance and Validation (CIAV)

Definition
A mission-based interoperability methodology that maps the end-to-end flow of information and exchange of data, assisting in the overall improvement, streamlining, and integration of processes involving operational and technical exchange requirements aligned to specific mission needs. The methodology results in fit for purpose determinations.

The process carried out by CIAV to analyze the execution of Coalition Mission Threads (CMT). It includes examination of operational information exchanges and associated processes. The end state is a report providing Capabilities and Limitations (CAPS/LIMS) supported by Operational Impact (OI) Statements. CIAV Process Phase 4 of 4.

Source
Derived from: Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5128.01, 1 October 2014 and Coalition Interoperability Assurance and Validation (CIAV) 101 Brief

See Also
Coalition Interoperability Assurance and Validation (CIAV) Request for Information (RFI)
Coalition Interoperability Assurance and Validation (CIAV) Requirement
Coalition Mission Thread (CMT)
Operational Requirements Master List (ORML)

Coalition Interoperability Assurance and Validation (CIAV) Recommendation

Definition
The suggestion to a CIAV customer on how to correct a Limitation or, if correction is not possible, on a viable workaround. Derived from the discovery of a limitation during a CIAV Desktop Analysis (DTA) or Assurance and Validation (A&V) event and is documented in a CIAV report.

Source
U.S. Coalition Interoperability Assurance and Verification (CIAV) Chief of Staff

Coalition Interoperability Assurance and Validation (CIAV) Request for Information (RFI)

Definition
The CIAV RFI is a form used to gather information necessary to capture the customer requirement(s) and identify critical information needed to support analysis and execute a successful CIAV Desktop Analysis (DTA) and possibly an Assurance and Validation (A&V) event, if it is required. CIAV Process Phase 2 of 4.

Source

Coalition Interoperability Assurance and Validation (CIAV) Request for Information (RFI) Standard Operating Procedure (SOP)

Coalition Interoperability Assurance and Validation (CIAV) Requirement

Definition
In terms of CIAV, a requirement is a coalition interoperability issue or challenge identified by the user that is presented to CIAV for possible analysis. The requirement must be validated and prioritized by the Mission Partner Environment Executive Steering Committee (ESC) or the North Atlantic Treaty Organization (NATO) Federated Mission Networking (FMN) governance body before CIAV can commit resources to analyze. Once validated and prioritized, it will be processed through CIAV, with a resulting CIAV recommendation for the user.

Source
Derived from: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5128 (Draft)

See Also
Coalition Interoperability Assurance and Validation (CIAV) Request for Information (RFI)
Mission Partner Environment Executive Steering Committee (MPE ESC) Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG)
Operational Requirements Master List (ORML)

Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG)

Definition
The international organization that addresses coalition interoperability issues and concerns, validated requirements, and event scheduling; an essential element in increasing interoperability within the affiliates by improving mission-based information exchange and driving resources to be used more effectively and efficiently. The U.S. is represented by U.S. CIAV.

Source
Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG) Calling Notice

See Also
Coalition Interoperability Assurance and Validation (CIAV) Requirement
Mission Partner Environment Executive Steering Committee (MPE ESC) Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG)
U.S Coalition Interoperability Assurance and Validation (CIAV)

Coalition Mission Thread (CMT)

Definition
An operational and technical description of the end-to-end set of activities and systems that accomplish the execution of a coalition mission as agreed upon by participating nations in a particular coalition operation.

Source
Derived from: Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01F, 21 March 2012 - definition for Joint Mission Thread and other sources

Coalition Network Operations Center (CNOC)/National Network Operations Center (NNOC)

Definition
Pegasus Service Operations Management constructs using the Information Technology Infrastructure Library (ITIL) process. The CNOC provides the coordinating guidance necessary to align Pegasus service operations functions of the NNOCs; whereas, the NNOCs provide Pegasus service operations within their respective national domain. The construct of an NNOC within sovereign boundaries remains the responsibility of an individual nation.

Source
Allied Communications Publication (ACP) 230, March 2015

See Also
Pegasus

Coalition Tactics, Techniques, and Procedures (CTTP)

Definition
Presents the end-to-end coalition mission thread performance criteria as agreed upon by coalition partners.

Source
Derived from: Joining, Membership, and Exiting Instructions (JMEI) v1.10, 11 August 2014

See Also
Coalition Mission Thread (CMT)

Coalition User

Definition
Any appropriately cleared individual relating to, belonging to, or representing a nation, who is a member of a coalition that has a requirement to access a mission enclave supporting that coalition.

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

Combined Enterprise Regional Information Exchange System (CENTRIXS)

Definition
A common set of networks built on a set of standard hardware, software, and services for U.S. and Coalition partner forces to share classified operational and intelligence information at the SECRET//Releasable (SECRET//REL) level. Each CENTRIXS network operates at a single security classification level and operates globally, regionally, and locally. The CENTRIXS environment is a combination of network and applications services. Most application services are provided by Commercial-Off-The-Shelf (COTS) products; a few Government-Off-The-Shelf (GOTS) solutions (e.g., guards; Intelligence, Surveillance, and Reconnaissance (ISR) capabilities) are used. CENTRIXS uses existing communications infrastructures such as the SECRET Internet Protocol Router Network (SIPRNET), whenever possible. The system employs National Security Agency (NSA)-approved Type-1 encryption devices to establish an encrypted channel between strategic or tactical locations and command headquarters sites and forward points of presence.

Source
Derived from: Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6285.01C, 15 May 2013 and Multinational Information Sharing (MNIS) Program Management Office (PMO) Systems Engineering Plan (SEP), 26 June 2014

Combined Enterprise Regional Information Exchange System - Maritime (CENTRIXS-M)

Definition
A CENTRIXS network managed by the U.S. Navy supporting Cooperative Maritime Forces Pacific which links the U.S. with Australia, Japan, Singapore, India, Korea and many other nations with Pacific navies.

Source
Derived from "CENTRIXS-Maritime: Connecting the Warfighter", CHIPS Magazine July–September 2011, A publication of the United States Department of the Navy Chief Information Officer, XXIX (III): 54–55, ISSN 1047-9988, OCLC 6062228

See Also
CENTRIXS

Combined Federated Battle Laboratories Network (CFBLNet)

Definition
A laboratory environment which utilizes a distributed Wide-Area Network used as the vehicle for network members (Combined Communications Electronics Board and North Atlantic Treaty Organization (NATO)), to experiment with new capabilities by conducting Research and Development, Trials and Assessment (RDT&A) initiatives.

Source
Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6285.01C, 15 May 2013

Combined Maritime Forces Central (CMFC)

Definition
A Type-2-protected Community-of-Interest (COI)/mission enclave, which uses Global Counter-Terrorism Forces (GCTF) network as their transport network, and the GCTF is interfaced with the CT core via High Assurance Internet Protocol Encryptor (HAIPE) devices.

Source
Allied Communications Publication (ACP) 200(D), Vol. 2, March 2015

Commercial Solutions for Classified (CSfC) Program

Definition
An NSA Central Security Services (CSS) program established to enable commercial products to be used in layered solutions protecting classified National Security System (NSS) data. This will provide the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years.

Source
National Security Agency (NSA) Commercial Solutions for Classified (CSfC) website

Reference
https://www.nsa.gov/ia/programs/csfc_program/

Common Mission Network Transport (CMNT)

Definition
An enterprise backbone infrastructure that will allow Combatant Commands/Services/Agencies (CC/S/A) to exchange and share information across regional operational network domains via the Defense Information Systems Network (DISN) backbone architecture without tunneling through layers of various transport. CMNT will provide a common transport for encrypted SECRET//Releasable (SECRET//REL) traffic to meet mission partner information sharing requirements.

A Layer 3 Virtual Private Network (VPN) service that provides mission partners the ability to connect to the Internet Protocol Transport-Provider Edge (IPT-PE) router or UNCLASSIFIED Provider Edge (UPE) router for the MPE-IS community. This VPN service provides Common Mission Network Transport (CMNT) mission partners the ability to obtain mission enclave access through the DoD's Multiprotocol Label Switching (MPLS) Layer 3 VPN at any Defense Security Service (DSS) location that includes IPT-PE or UPE IP Data access.

Source
Derived from: Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6285.01C, 15 May 2013 and Defense Information Systems Agency (DISA) Common Mission Network Transport (CMNT) website, http://www.disa.mil/Network-Services/VPN/CMNT; Accessed: 30 September 2015

Community of Interest (COI)

Definition
A collaborative group of users within a mission enclave who 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. All COIs within a mission enclave operate within the same security domain as the mission enclave, but may employ access controls to manage COI membership.

Source
Derived from: Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015

See Also
Mission Partner Environment – Information System (MPE-IS) Mission Enclave

Cooperative Maritime Forces Pacific (CMFP)

Definition
A Combined Enterprise Regional Information Exchange System (CENTRIXS) effort in the Pacific area of responsibility that links the U.S. with Australia, Japan, Singapore, India, Korea and many other nations involved in exercises or operations in the Pacific. CMFP is a Type-2-protected Community of Interest (COI), which uses the Global Counter-Terrorism Forces (GCTF) network as their transport network, and the GCTF is interfaced with the CT core via High Assurance Internet Protocol Encryptor (HAIPE) devices.

Source
Derived from: Dakis, Ann. "CENTRIXS-Maritime: Connecting the Warfighter", CHIPS Magazine July–September 2011, A publication of the U.S. Department of the Navy Chief Information Officer, XXIX (III): 54–55, ISSN 1047-9988, OCLC 60622282 and Allied Communications Publication (ACP) 200(D), Vol. 2, March 2015.

See Also
Combined Enterprise Regional Information Exchange System (CENTRIXS)

Core Data Center (CDC)

Definition
A CDC is a fixed DoD data center meeting DoD standards for facility and network infrastructure, cybersecurity, technology, and operations and adhering to enterprise governance. Functions and services delivered by current DISA DECCs, Component Enterprise DCs and Component Installation DCs will be consolidated to the greatest extent possible into Core DCs totaling a few dozen at most. CDCs will be selected from existing Component data centers.

Source
DoD Data Center Reference Architecture Version 1.10, 25 April 2014

Core Mission Partner Environment- Information System (MPE-IS) SECRET//Releasable Services

Definition
The minimum set of IT and Command and Control (C2) services required by MPE-IS SECRET//Releasable (SECRET//REL) mission enclaves. These services are: Email (with attachments), Chat, Full Motion Video (FMV), Geo-Situational Awareness/Common Operational Picture (COP), Video Teleconferencing (VTC), Voice, Web/File Share, Directory/Global Address List (GAL) look-up, Office Automation, Print, Classification tool, Organizational Messaging, and Language Translation.

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

Cross Domain

Definition
The act of manually and/or automatically accessing and/or transferring information between different security domains.

Source
Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015

Cross Domain Controlled Gateway (CDCG)

Definition
The CDCG component functions as a Cross Domain Solution (CDS) that supports the controlled transfer of data from one security domain to another. It provides information sharing services for an operational domain.

Source
DoD Cybersecurity Reference Architecture (CS RA) Version 3.0 (FINAL), 24 September 2014

Cross Domain Enterprise Services (CDES)

Definition
DISA Cross Domain Enterprise Service (CDES) provides support to Combatant Commands, Services, and Agencies by implementing, fielding, and providing lifecycle support for cross domain solution technologies that provide secure interoperable capabilities throughout the Department of Defense. DISA provides consolidated cross domain solutions on behalf of DoD components and develops a robust cross domain fielding capability under the Chairman Joint Chiefs of Staff Instruction (CJCSI) 6211.02D.

Source
DISA web site (http://www.disa.mil/Cybersecurity/Cross-Domain-Enterprise-Services)

Cross Domain Solution (CDS)

Definition
A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.

Source
Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015

2.4 D-Terms

Data Center Virtualization (DCV)

Definition
The activity of implementing a Mission Partner Environment – Information System (MPE-IS) Virtual Data Center (VDC).

Note: The preferred term is VDC when referring to the tangible implementation that results from DCV.

Source
Derived from: Mission Partner Environment – Information System (MPE-IS) Virtual Data Center (VDC) Service Description, Version 0.8, 1 February 2016

See Also
Virtual Data Center (VDC)

Defense Information Systems Network (DISN)

Definition
The integrated network centrally managed and configured by the Defense Information Systems Agency to provide dedicated point-to-point, switched Voice and Data, Imagery, and Video Teleconferencing services for all DoD activities.

Source
Joint Publication 1-02, 15 June 2015

Defense Support of Civil Authorities (DSCA)

Definition
Support provided by federal military forces, DoD civilians, DoD contract personnel, DoD component assets, and National Guard (NG) forces (when the Secretary of Defense (SecDef), in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, U.S. Code status or when federalized) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.

Source
Joint Publication 3-28, Defense Support of Civil Authorities (DSCA), 31 July 2013

Defensive Cyberspace Operations (DCO)

Definition
Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.

Source
Joint Publication (JP) 3-12, Cyberspace Operations, 5 February 2013

Department of Defense Information Network (DoDIN)

Definition
The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

Source
Joint Publication 1-02, 15 June 2015

Department of Defense Information Network (DoDIN) Operations

Definition
Actions taken to design, build, configure, secure, operate, maintain, and sustain DoD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. These include proactive actions, which address the entire DoDIN, including configuration control and patching, Information Assurance (IA) measures and user training, physical security and secure architecture design, operation of host-based security systems and firewalls, and encryption of data.

Source
Joint Publication (JP) 3-12, Cyberspace Operations, 5 February 2013

Department of Defense Partnered Systems

Definition
Information Systems (IS) or Platform Information Technology systems that are developed jointly by DoD and non-DoD mission partners, comprise DoD and non-DoD ISs, or contain a mix of DoD and non-DoD information consumers and producers (e.g., jointly developed systems, multinational or coalition environments, or first responder environments).

Source
DoD Instruction (DoDI) 8500.01, 14 March 2014

Director of Military Support (DOMS)

Definition
The State National Guard officer responsible for coordinating Defense Support of Civil Authorities (DSCA), providing oversight for domestic operations and providing prepared units to mitigate incident impacts in the State or in the U.S. at the direction of appropriate civil authorities.

Source
National Guard Bureau (NGB) Lexicon, as presented at the Senior Engineering Working Group (SEWG) Meeting on 6 August 2015

See Also
Defense Support of Civil Authorities (DSCA)

Domain

Definition
An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Note: In an MPE-IS context, the preferred term is “Mission Enclave”

Source
Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015

Domestic Operations (DOMOPS)

Definition
Collective reference for Defense Support of Civil Authorities (DSCA), National Guard Civil Support (NGCS), and National Guard Domestic Operations (NGDO). Generally speaking, those are DoD enabled or otherwise supported missions or tasks, performed within the 48 Continental United States, Alaska, Hawaii, the U.S. Territories (Guam, Puerto Rico, U.S. Virgin Islands), or the District of Columbia. DOMOPS are carried out at the direction of appropriate civil authorities.

Source
Joint Publication (JP) 1-02, 15 June 2015 and National Guard Regulation (NGR) 500-1

See Also
Defense Support of Civil Authorities (DSCA)

2.5 E-Terms

Emergency Management Constellation (EM Constellation)

Definition
A web-based application and Structured Query Language Server database hosted within the State of Florida Division of Emergency Management Data Center (disaster recovery/failover/Continuity of Operations at Camp Blanding, Florida, also Internet accessible). The system allows the State Emergency Response Team (SERT), composed of county, state, federal, volunteer, and mutual aid entities, to use the same operating environment when responding to and recovering from an emergency.

Source
State of Florida Division of Emergency Management briefing provided to the Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG) in August 2015

Enclave

Definition
A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. 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.

Note: In an MPE-IS context, the preferred term is “Mission Enclave”

Source
Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015 and DoD Instruction (DoDI) 8330.01, 21 May 2014

Enduring Mission Partner Environment – Information System (MPE-IS) Mission Enclave

Definition
A persistent information sharing and data exchange capability (mission enclave) that provides a multi-level security system capable of tagging and labeling information with applicable classification markings making that data available only to those with appropriate clearance, access, and need to know.

Attributes:
i. Strategic Level (planning)
ii. Persistent – time not a factor
iii. Specified Mission Partners (MPs) (bi-lateral or multi-lateral "mission enclaves")
iv. Combatant Command Headquarters capabilities for Mission Partner engagement/planning
v. Technologically dependent
vi. Integrated with and enabled by the Joint Information Environment (JIE)
vii. May be used to conduct operations when Episodic MPE-IS is not desirable or feasible

Source
Derived from**:** U.S. DoD Episodic Mission Partner Environment Joining Instructions, Version 1.10, 11 August 2014

Enterprise Cross Domain Services (ECDS)

Definition
A set of services that facilitates secure information sharing across security domains operating at different classification and releasability levels for DoD and its mission partners. ECDS enables the cross domain transfer of a variety of file types and transfer protocols within a secure, consolidated, highly available streamlined enterprise environment. ECDS provides an automated alternative to the use of removable media for cross domain transfers, as well as facilitates the reduced proliferation of high-risk, costly, disparate point-to-point devices community wide.

Source
Derived from: Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015 and Defense Information Systems Agency (DISA) ID32 Cross Domain Enterprise Service (CDES)

Episodic Mission Partner Environment – Information System (MPE-IS) Mission Enclave

Definition
[Typically] temporary in planned duration and formed to support a specific mission (Conflicts, Humanitarian Assistance, Disaster Response, Stability Operations, etc.) at the operational/tactical level.

An Episodic MPE-IS mission enclave will provide a multi-lateral, "fight tonight" capability able to expand and or contract mission enclaves on demand. In some cases, an Enduring MPE-IS mission enclave will support an episodic mission enclave.

An episodic mission enclave leverages a federated network concept supporting the connection of multiple networks and national systems, with applications and tools, to enable mission partner information-sharing within a single information environment. Episodic mission enclaves require MPs to contribute a mission-specific set of computing resources with the full set of core capabilities (including direct Voice over

Internet Protocol (VoIP) and Video Teleconferencing (VTC)), tactical access, and required mission applications.

Attributes:
i. Temporal – time to establish/operate always a factor
ii. Mission focused (exercise or contingency operation)
iii. Unknown mission partners, emergent mission; unknown duration
iv. Joint Task Force capabilities for Mission Partner operations
v. Leverages federation of partner capabilities
vi. U.S. may not be the lead; but U.S. forces must leverage JIE

Source
Derived from: U.S. DoD Episodic Mission Partner Environment Joining Instructions, Version 1.10, 11 August 2014

Extended Network Mission Partner (ENMP)

Definition
A mission partner that connects a network extension to a Network Contributing Mission Partner (NCMP) network contribution for information sharing and data exchange.

Source
U.S. DoD Episodic Mission Partner Environment Joining Instructions, Version 1.10, 11 August 2014

2.6 F-Terms

Federal Agency Partner

Definition
Any appropriately cleared Federal agency partner with a requirement to access a DoD information system for performing or assisting in a lawful and authorized governmental function.

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

Federated Service Configuration

Definition
One of the three service configuration options for Mission Partner Environment – Information System (MPE-IS). The Federated Service Configuration supports several different partner countries with their own application services by enabling interconnection of their national services with DoD MPE-IS services.

Source
Derived from: Mission Partner Environment – Information System Reference Architecture (MPE-IS RA), Ver. 1.00, 23 March 2016 and other sources

Federated Mission Network (FMN)

Definition
The collection of connected networks provided by MPs. Common information domain extending across all network extensions at a single security level.

Source
Joining, Membership, and Exit Instructions (JMEI) Version 1.10, 11 August 2014

See Also
Network Contributing Mission Partner (NCMP)

Federated Mission Networking (FMN)

Definition
North Atlantic Treaty Organization (NATO) term for a governed conceptual framework consisting of people, processes, and technology to plan, prepare, establish, use, and terminate Mission Networks in support of federated operations.

Source
North Atlantic Treaty Organization (NATO) Federated Mission Networking Implementation Plan, Volume I, 11 August 2014

Federated Mission Networking (FMN) Framework

Definition
North Atlantic Treaty Organization (NATO) term for a governed, managed, all-inclusive structure providing processes, plans, templates, enterprise architectures, capability components and tools needed to plan, prepare, develop, deploy, operate, evolve, and terminate Mission Networks in support of Alliance and multinational operations in dynamic, federated environments.

Source
North Atlantic Treaty Organization (NATO) Federated Mission Networking Implementation Plan, Volume I, 11 August 2014

Federation

Definition
A federation is a collection of distinct entities that have agreed to work together to achieve a common goal that could not be achieved by any one entity on its own. In a federation, each entity retains its identity and responsibility for its contribution to the federation, while adhering to an agreed-upon set of rules, standards, and protocols for the operation of the federation as a whole. Each entity can be both a producer and a consumer of information generated within the federation. In comparison, in integration, the individual entities are subsumed into a new whole and the identities and roles of the original entities are lost.

Source
Mission Partner Environment – Information System Reference Architecture (MPE-IS RA), Ver. 1.00, 23 March 2016

Federation - North Atlantic Treaty Organization (NATO)

Definition
An association of NATO, NATO nations and non-NATO entities participating in missions, each retaining control of their own capabilities and affairs while accepting and complying with the requirements as laid out in the pre-negotiated and agreed arrangements.

Source
North Atlantic Treaty Organization (NATO) Federated Mission Networking Implementation Plan, Volume I, 11 August 2014

Five Eyes (FVEY)

Definition
The "Five Eyes," often abbreviated as "FVEY," refer to an alliance comprising Australia, Canada, New Zealand, the United Kingdom (UK), and the United States (USA). These countries are bound by a multi-lateral Agreement/treaty for joint cooperation.

Source
Derived from: Various Combined Communication Electronics Board (CCEB) documents

Foreign Humanitarian Assistance (FHA)

Definition
Department of Defense activities conducted outside the United States and its territories to directly relieve or reduce human suffering, disease, hunger, or privation.

Source
Joint Publication (JP) 3-29, 3 January 2014

Foreign Disaster Relief (FDR)

Definition
Assistance that can be used immediately to alleviate the suffering of foreign disaster victims that normally includes services and commodities as well as the rescue and evacuation of victims; the provision and transportation of food, water, clothing, medicines, beds, bedding, and temporary shelter; the furnishing of medical equipment, medical and technical personnel; and making repairs to essential services.

Source
Joint Publication (JP) 3-29, 3 January 2014

2.7 G-Terms

Gateway (GW)

Definition
An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.

The interconnection between two networks with different communications protocols. Gateways operate at the fourth through seventh layers of the Open System Interconnection model.

Source
Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015 and Allied Communications Publication (ACP) 122(G), February 2015

Geospatial Assessment Tool for Operations and Response (GATOR)

Definition
The Common Operational Picture (COP)/situational awareness viewer used by the State of Florida.

Source
State of Florida Division of Emergency Management briefing provided to the Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG) in August 2015

2.8 H-Terms

Geospatial Information Interoperability Exploitation Portable (GIIEP)

Definition
The Geospatial Information Interoperability Exploitation - Portable (GIIEP) system is a man-portable, multi-band receiver capable of ingesting a variety of visual and textual data to enhance the ability to respond to disaster situations and provide annotated and compressed imagery products (both still and video) that can be quickly disseminated to mission partners. The inherent flexibility of the system allows operators to tailor their efforts to take maximum advantage of available assets and available communications as they support disaster response operations. GIEEP was developed by the U.S. Army Space and Missile Defense Command as a client-server application based on Government-Off-The-Shelf (GOTS) and non-proprietary software. GIEEP connects directly to Google Earth Enterprise (GEE). Client-side user functions include Global Positioning System (GPS) status, chat, photograph capture and sharing, and a capability to send full motion video to the GIIEP server.

Source
Derived from: GIEEP Users Guide and other sources

Global Command and Control System (GCCS)

A deployable command and control system supporting forces for joint and multinational operations across the range of military operations with compatible, interoperable, and integrated communications systems. Also called GCCS. GCCS incorporates systems that provide situational awareness, support for intelligence, force planning, readiness assessment, and deployment applications that battlefield commanders require to effectively plan and execute joint military operations.

Source
Derived from: Joint Pub (JP) 6-0, Joint Communications System and other sources

High Assurance Controlled Interface (HACI)®

Definition
HACI® devices provide the physical connection boundaries to any number of security domains, using one device per domain.

A security domain is a unique bi-lateral or multi-lateral network, developed and maintained through information sharing policies and various agreements between the U.S. and its partner nations. The joining rules include appropriate approvals found in the National Disclosure Policy and Intelligence Sharing Agreements, including technical and security agreements, et al. Once approvals are in place, a configured HACI® becomes the physical boundary device between a partner nation's network and the Trusted Network Environment® (TNE®).

Source
U.S. Battlefield Information Collection and Exploitation Systems – Extended (U.S. BICES-X) Trusted Network Environment® Technology Information Paper, November 2013

High Assurance Internet Protocol Encryptor (HAIPE)

Definition
A Type 1 encryption device that complies with the National Security Agency's HAIPE Interoperability Specification (IS) (formerly the HAIPIS, the High Assurance Internet Protocol Interoperability Specification). HAIPE devices provide networking, traffic protection, and management features that provide Information Assurance (IA) [cybersecurity] services for IPv4/IPv6 networks.

Source
Committee on National Security Systems Policy (CNSSP) No. 19, 10 June 2013

Homeland Defense (HD)

Definition
The protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats as directed by the President.

Source
Joint Publication (JP) 1-02, 15 June 2015

Homeland Defense Activity (HDA)

Definition
An activity undertaken for the military protection of the territory or domestic population of the United States, or of infrastructure or other assets of the United States determined by the Secretary of Defense as being critical to national security, from a threat or aggression against the United States.

Source
Title 32, U.S. Code, Section 901

Homeland Security Information Network (HSIN)

Definition
A trusted network and application that is managed, operated, and maintained by the U.S. Department of Homeland Security. The system is intended for homeland security mission operations, for the purpose of sharing Sensitive But UNCLASSIFIED (SBU) information among authorized mission partners. Federal, State, Local, Territorial, Tribal, International, and Private Sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.

Source
Department of Homeland Security's Homeland Security Information Network (HSIN) website

Reference
https://www.dhs.gov/homeland-security-information-network-hsin

Hosted Mission Partner (HMP)

Definition
Mission partner that is embedded within a Network Contributing Mission Partner (NCMP)/Extended Network Mission Partner (ENMP) network.

Source
U.S. DoD Episodic Mission Partner Environment Joining Instructions, Version 1.10, 11 August 2014

See Also
Network Contributing Mission Partner (NCMP)
Extended Network Mission Partner (ENMP)

Hypervisor

Definition

Privileged system software, like an operating system, that logically partitions a single physical computer system into one or more virtual machines and shares its physical host computer with a virtual machine.

Source
The Next Wave, Volume 18, Number 4, 2011, The Security Impact of System Virtualization

2.9 I-Terms

Identity and Access Management (IdAM)

Definition
Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and Non-Person Entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources.

Source
Derived from: Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015

Incident Awareness and Assessment (IAA)

Definition
The Secretary of Defense approved use of Department of Defense intelligence, surveillance, reconnaissance, and other intelligence capabilities for domestic non-intelligence support for defense support of civil authorities.

Source
Joint Publication (JP) 1-02, 15 June 2015

Information Control Domain (ICD)

Definition
A set of information content and associated processes and activities that fall under a specific set of policies directing sharing restrictions, protection measures, handling instructions and other similar documents.

An ICD is labeled and characterized by markings in accordance with the [Security Markings Program] (formerly Controlled Access Program Coordination Office (CAPCO)). Each "releasable to" caveat labels an ICD including bi-lateral releasability (e.g., SECRET//Releasable (SECRET//REL) KOR) and multi-lateral as characterized by a [Security Markings Program] tetragraph (e.g., SECRET//REL UNCK). An ICD Authority (ICDA) has the stewardship and expertise to manage, approve, deny, and make exceptions to the associated policy. An ICD refers to information content.

Source
Cieslak, Randall (U.S. Pacific Command (PACOM) Chief Information Officer (CIO)), "Network Design proposal for the JIE and the MPE," Version 1.1, 14 November 2013

Information Exchange Requirement (IER)

Definition
Operational IER: Established information parameters, theater or situationally derived, in an operational environment that satisfy or define the Services that comprise a specific Mission Thread.

System IER: Also known as a System Exchange Requirement (SER), identifies the system data exchanged between nodes, systems at the nodes, and information riding the systems' interfaces.

Source
Derived from: Coalition Mission Threads and Their Associated Services for the Mission Partner Environment (MPE) and Federated Mission Network (FMN) and the DoD Architecture Framework (DoDAF) SV-6.

Information Sharing

Definition
Making information available to participants (people, processes, or systems). Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant.

Source
DoD Information Sharing Strategy, 4 May 2007

Installation Processing Node (IPN)

Definition
An IPN is a fixed DoD data center serving a single DoD installation and local area (installations physically or logically behind the network boundary) with local services that cannot be (technically or economically) provided from a CDC. Each IPN may have multiple physical enclaves (managed as a single virtual IPN) to accommodate unique installation needs (e.g., Joint Bases).

Source
DoD Data Center Reference Architecture Version 1.10, 25 April 2014

Internet Access Point (IAP)

Definition
A network exchange facility where Internet Service Providers (ISPs) connect with the DoD networks in a peering arrangement. The connections within IAPs determine traffic routing to DoD networks and the Internet.

Source
Joint Information Environment (JIE) Unified Capabilities (UC) Solution Architecture

Interoperability

Definition
The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.

Source
Joint Publication (JP) 1-02, 15 June 2015

2.10 J-Terms

Joining, Membership, and Exiting Instructions (JMEI)

Definition
Network standards for partners joining a U.S., DoD-led mission enclave. The processes and technical configurations required of Mission Partners (MPs) when connecting an MP or national network extension

to an event lead’s mission network core at a security classification level specific to that event, proposing and implementing changes to services operating within the mission network, and when disconnecting a national extension from a mission network core. The intent of the JMEI is to provide a template for connection of joint services and MPs in a trusted federated mission network that is consistent and coherent across the DoD. JMEI may be utilized as a template to guide establishment of a federation of networks to support any event with a unique security classification level information and data exchange environment shared by all MPs electing to connect.

Source
DoD Instruction (DoDI) 8110.01, 6 February 2004 and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5128.01, 1 October 2014

Joint Information Environment (JIE)

Definition
A secure [DoD] environment, comprised of shared Information Technology (IT) infrastructure, enterprise services, and single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per Unified Command Plan using enforceable standards, specifications, and common Tactics, Techniques, and Procedures (TTPs).

Source
Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5128.01, 1 October 2014

Joint Information Environment (JIE) Technical Synchronization Office (JTSO)

Definition
A joint organization hosted by the Defense Information Systems Agency (DISA). DISA has been given responsibility for the technical aspects of JIE and leads the JTSO, which includes DISA staff, as well as representation from the military services, intelligence community, and National Guard. JTSO's mission is to serve as the Technical and Implementation Lead for the JIE and provide a single, secure, reliable, timely, effective, and agile enterprise information environment for use by Joint forces and non-DoD mission partners.

Source
Derived from: Joint Information Environment (JIE) Executive Committee (EXCOM) briefing: “DoD IT Effectiveness - Building the Joint Information Environment to Enable Full Spectrum Dominance,” 18 July 2012

Joint Regional Security Stack (JRSS)

Definition
A suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, Virtual Routing and Forwarding (VRF) and provides a host of network security capabilities. Each physical stack is comprised of racks of equipment, which enable big data analytics, allowing DoD components to intake large sets of data to the cloud and provide the platforms for processing data, as well as the mechanism to help analysts make sense of the data.

JRSS allows information traversing DoD networks to be continuously monitored to ensure response time as well as throughput and performance standards. JRSS includes failover, diversity, and elimination of critical failure points as a means to assure timely delivery of critical information.

Source

Defense Information Systems Agency (DISA) Joint Regional Security Stacks (JRSS) Portal

Reference
http://www.disa.mil/Initiatives/JRSS

2.11 L-Terms

Language Translation

Definition
Provides the ability to render something written or spoken in one language in words of a different language; to translate data/information between two or more partners that have different languages to obtain common understanding. Mission Partner Environment – Information System (MPE-IS) has identified Language Translation as a required service.

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

Law Enforcement Online - Enterprise Portal (LEO-EP)

Definition
A free, secure, Web-based information system that is managed, operated, and maintained by the Federal Bureau of Investigation (FBI) for use by authorized members of the law enforcement community. Services currently available to authorized users via the LEO-EP include: Regional Information Sharing System (RISS)—A system that provides timely access to a variety of criminal intelligence databases; Intelink—A secure portal for integrated intelligence dissemination and collaboration efforts; National Data Exchange (N-DEx) —A powerful, investigative tool that provides law enforcement agencies with the ability to search, link, analyze, and share criminal justice information; Joint Automated Booking System (JABS) —A repository of federal arrest information; Internet Crime Complaint Center (IC3) —A vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber-crime; National Gang Intelligence Center—A multi-agency effort that integrates gang information from local, state, and federal law enforcement entities to serve as a centralized intelligence resource for gang information and analytical support; and U.S. Department of Justice Information Data Exchange Architecture (IDEA) my FX—A Web-based capability that allows files/folders to be securely transferred among cross-organizational teams. LEO-EP services also include Email, Virtual Office, Virtual Command Center, Special Interest Groups, Forums, and a Library.

Source
Federal Bureau of Investigation (FBI) Law Enforcement Online – Enterprise Portal (LEO-EP) Website

Reference
https://www.cjis.gov/CJISEAI/EAIController

Limitations (LIMS)

See Capabilities/Limitation, Operational Impacts (CAPS/LIMS, OIs).

2.12 M-Terms

Minimum Implementation (MinImp)

Definition

The statement of the minimum data exchange requirements that must be implemented to ensure a minimum level of interoperability at the operator level. Any message, case, and data element that is required to be implemented by all systems.

Source
Military Standard (MIL-STD) 6016E, 20 July 2012, Table 3.3-1 and Military Standard (MIL-STD) 6017C, 31 May 2012, §3.2

Minimum Operational Requirement (MOR)

Definition
The baseline whereby interoperability exists across coalition standards, and capabilities and limitations are documented for use in planning and assessment efforts.

The performances and their associated metrics and criteria established by the commander of an operational mission as the essential capabilities required to execute that mission.

Source
Coalition Interoperability Assurance and Validation (CIAV) Mission Thread Anatomy and Coalition Interoperability Assurance and Validation (CIAV) Mission Profiles Implementation Strategy

Reference
Joint Publications (JP): https://jdeis.js.mil/jdeis/index.jsp?pindex=43

Mission

Definition
The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.

Source
Joint Publication (JP) 1-02, 15 June 2015

Mission-Based Interoperability (MBI)

Definition
End-to-end interoperability among all elements of a coalition – from producers to consumers.

Source
Using Coalition Interoperability Assurance and Validation (CIAV) to Achieve Mission-Based Interoperability, 2 December 2013

Mission Partner (MP)

Definition
Those with whom the DoD 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.

Source
DoD Instruction (DoDI) 8110.01, 6 February 2004

Mission Partner Environment (MPE)

Definition
An operating environment that enables Command and Control (C2) for operational support planning and execution on a network infrastructure at a single security level with a common language. An MPE

capability provides the ability for Mission Partners (MPs) to share their information with all participants within a specific partnership or coalition beginning in Phase 0 and transitioning to execution of Phase 1, Day 1 operations.

Source
DoD Instruction (DoDI) 8110.01, 6 February 2014

Mission Partner Environment Executive Steering Committee (MPE ESC)

Definition
A Flag Officer/General Officer (FO/GO) level joint body to govern and manage the MPE framework.

Source
Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5128.01, 1 October 2014

Mission Partner Environment Executive Steering Committee (MPE ESC) Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG)

Definition
A compilation of members who create a collaborative environment as organizations engage due to their need in addressing interoperability issues; an alliance of organizations whose primary mission is to address interoperability shortfalls which continue to challenge Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance (C5ISR) operations. It is led by an O-6 level individual assigned by the Defense Information Systems Agency (DISA), and membership is comprised of O-6 level representatives from Office of Secretary of Defense (OSD), the Joint Staff, the Combatant Commands, the Services, and other relative organizations. The MPE ESC CIAV WG Lead directs U.S. CIAV to address MPE ESC-validated requirements.

Source
Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5128 (Draft)

See Also
Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG)
U.S. Coalition Interoperability Assurance and Validation (CIAV)

Mission Partner Environment – Information System (MPE-IS)

Definition
The materiel (M) element of the DOTMLPF-P framework. It depicts an agile and flexible technical foundation for improving mission execution to meet dynamic mission requirements with diverse partners. MPE-IS capabilities are an extension of Joint Information Environment (JIE) capabilities. MPE-IS is coupled with non-materiel elements of the framework to meet overall objectives for the MPE vision.

Note: DOTMLPF-P: Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

Mission Partner Environment – Information System (MPE-IS) Client

Definition
An end-user computing device that connects a user to one or more mission enclaves containing information and services specific to those mission enclaves. The range of devices and technologies include thick client workstations and laptops operating in a client-server architecture, thin (or zero) client terminals operating in a Virtual Desktop Infrastructure (VDI) architecture, multi-enclave clients, and mobile clients (e.g., tablets and smartphones).

Source
Mission Partner Environment – Information System Reference Architecture (MPE-IS RA), Ver. 1.00, 23 March 2016

Mission Partner Environment – Information System (MPE-IS) Expeditionary Node

Definition
A non-fixed, deployable set of capabilities that provides MPE-IS Virtual Data Center (VDC) services to tactical/expeditionary users. An expeditionary node will typically be installed at a Joint Information Environment (JIE) Tactical Processing Node (afloat, ashore, or airborne).

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

See Also
Mission Partner Environment – Information System (MPE-IS) Global Node
Mission Partner Environment – Information System (MPE-IS) Global Node Extension

Mission Partner Environment – Information System (MPE-IS) Global Node

Definition
Consists of the capabilities required to provide MPE-IS Virtual Data Center (VDC) services to users within one or more regions (e.g., U.S. European Command (EUCOM) Area of Responsibility (AOR), U.S. Central Command (CENTCOM) AOR). Six global nodes are planned, two in the Continental U.S. (CONUS) and four Outside the Continental U.S. (OCONUS). Global node capabilities include the provisioning of on-demand, classification-specific, mission enclaves enabled with Virtual Desktop Infrastructure (VDI), Core Services (e.g., Email, Chat, Video Teleconferencing (VTC)), Command and Control (C2) mission services, and support services (e.g., Directory, Information Technology Service Management (ITSM), Office Automation). Global nodes will typically be installed at Joint Information Environment (JIE) Core Data Centers (CDCs).

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

See Also
Mission Partner Environment – Information System (MPE-IS) Global Node Extension
Mission Partner Environment – Information System (MPE-IS) Expeditionary Node

Mission Partner Environment – Information System (MPE-IS) Global Node Extension

Definition

Consists of the capabilities required to provide MPE-IS Virtual Data Center (VDC) services to users within a specified sub-region (e.g., U.S. Forces Korea (USFK) Area of Responsibility (AOR)) with the node located in that sub-region. A global node extension is intended to address the resiliency needs of providing VDC services to users that operate in Disconnected, Intermittent, and/or Limited bandwidth (DIL) environments. Extension nodes will typically be installed at Joint Information Environment (JIE) Core Data Centers (CDCs) or Installation Processing Nodes.

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

See Also
Mission Partner Environment – Information System (MPE-IS) Global Node
Mission Partner Environment – Information System (MPE-IS) Expeditionary Node

Mission Partner Environment – Information System (MPE-IS) Mission Enclave

Definition
A governed, virtual mission execution environment that enables trusted, secured, assured and agile information sharing without impediment between specified mission participants. A mission enclave consists of standards-based capabilities and services that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Source
Derived from: Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015

See Also
Enclave
Domain
Agile Virtual Enclave (AVE)
Federated Mission Networking (FMN)

Mission Partner Environment – Information System (MPE-IS) Mission Enclave Resiliency

Definition
All the capabilities associated with Continuity of Operations and Disconnected, Intermittent, and/or Low Bandwidth (DIL) environments supporting MPE-IS users within mission enclaves.

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

Mission Partner Environment – Information System (MPE-IS) Multi-Enclave Client (MEC)

Definition
A Multilevel Secure (MLS) desktop implementation leveraging Virtual Desktop Infrastructure (VDI) technology that provides users with access to multiple mission enclaves (multiple security domains) on a single computing device.

Source

Derived from: Cieslak, Randall (U.S. Pacific Command (PACOM) Chief Information Officer (CIO)), "Network Design proposal for the JIE and the MPE," Version 1.1, 14 November 2013

See Also
Mission Partner Environment – Information System (MPE-IS) Multi-Enclave Client (MEC) Services

Mission Partner Environment – Information System (MPE-IS) Multi-Enclave Client (MEC) Services

Definition
A Local Area Network (LAN) or a set of computers attached to the network environment that provides users with network access and computing capability. MEC Services support MECs with Internet Protocol Security (IPSec) encryption built into the client, and either separate virtual machines are used to connect to each network security enclave, or served images are provided as instantiated by a desktop virtualization engine. The goal of the network is to enable the user with one device to access all the security enclaves needed by and authorized for the user.

Source
Derived from: Cieslak, Randall (U.S. Pacific Command (PACOM) Chief Information Officer (CIO)), "Network Design proposal for the JIE and the MPE," Version 1.1, 14 November 2013

See Also
Mission Partner Environment – Information System (MPE-IS) Multi-Enclave Client (MEC)

Mission Partner Environment–Information System (MPE-IS) Senior Engineering Working Group (SEWG)

Definition
Responsible for the development of the materiel solutions needed to transform the MPE to the approved vision for 2021. The MPE-IS SEWG nominally operates under the governance of the MPE Executive Steering Committee (ESC), but the SEWG Chair reports to the DoD Chief Information Officer (CIO). The MPE-IS SEWG is led by a member of the Senior Executive Service, who reports directly to the DoD CIO. The SEWG membership includes action officer-level representatives from the Combatant Commands, Military Departments, DoD CIO, the Joint Chiefs of Staff, the Defense Information Services Agency (DISA), National Guard Bureau (NGB), and National Security Agency (NSA).

Source
Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

See Also
Mission Partner Environment Executive Steering Committee (MPE ESC)

Mission Partner Environment – Information System (MPE-IS) Transport, Global Gray Core (GGC)

Definition
An interoperable, reliable/distributed, and cost-effective centralized Virtual Private Network (VPN) and certificate management capability that encapsulates the Joint Information Environment (JIE) technical solution to improve information exchange security between mission partners operating within the MPE and U.S. forces operating within the JIE. The MPE-IS Transport GGC is needed to secure classified (SECRET//Releasable (SECRET//REL)) bi-lateral and multi-lateral Mission Partner Gateway – Extended (MPGW-X) traffic over the Defense Information Systems Agency (DISA)-provided Common Mission

Network Transport (CMNT) and other non-DoD networks connected to the National Network Interface (NNI) of the Partner National Gateway using National Security Agency (NSA)-approved Commercial Solutions for Classified (CSfC) VPN Capability Package (CP).

A Gray Network is defined as a network where all classified data is protected by one layer of approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. A Gray Network exists between a secure Red Network (e.g., the SECRET Internet Protocol Router Network (SIPRNET)) and an untrusted Black Network (e.g., the Internet). A Gray Network is considered a Sensitive But UNCLASSIFIED (SBU) network, but it must be physically protected as a classified network. A single Gray Network can connect to multiple classified networks enabling domain specific computers access to either SIPRNET or Coalition classified networks through one common infrastructure. Client services (like Email, Portal, and Voice/Video) are not provided by a Gray Network, since it is principally a connection/transport network, allowing authenticated devices to connect and transit the Gray environment reroute to their Red Network domain. Additionally, Security Information and Event Management (SIEM) tools must be used to monitor and protect the Gray Network, because it provides the buffer between the classified networks and the untrusted internet.

Source
Derived from: National Security Agency (NSA) Information Assurance Directorate (IAD) Commercial Solutions for Classified (CSfC) Capability Package, 2015 and Mission Partner Environment – Information System (MPE-IS) Global Gray Core (GGC) Service Description, Version 0.4, 29 January 2016

See Also
Common Mission Network Transport (CMNT)
Commercial Solutions for Classified (CSfC) Program

Reference
National Security Agency (NSA) Commercial Solutions for Classified (CSfC) website, https://www.nsa.gov/ia/programs/csfc_program/

Mission Partner Gateway – Extended (MPGW-X)

Definition
The gateway through which bi-lateral and multi-lateral Mission Partners will communicate with the Joint Information Environment (JIE). The MPGW-X encapsulates hardware/software systems that route network traffic and services between JIE and mission partner networks. The MPGW-X is one of several technical components within the Mission Partner Environment.

Source
Mission Partner Gateway – Extended (MPGW-X) Service Description (SD), Version 2.2, 22 February 2016

Mission Partner Gateway – SECRET (MPGW-S)

Definition
One of four shared situational awareness components that define and enforce the boundary between the Joint Information Environment (JIE) and the external environment. MPGW-S is the gateway for SECRET mission partner networks such as U.S. Federal partners and FVEY partners.

Source
Mission Partner Gateway – Extended (MPGW-X) Service Description (SD), Version 2.2, 22 February 2016

Mission Partner Gateway – UNCLASSIFIED (MPGW-U)

Definition
A gateway through which Mission Partners (MPs) will communicate UNCLASSIFIED information with Joint Information Environment (JIE). The MPGW-U encapsulates hardware/software systems that route network traffic and services between JIE and mission partner networks. The MPGW-U is one of several technical components within the Mission Partner Environment.

Source
Mission Partner Gateway – Extended (MPGW-X) Service Description (SD), Version 2.2, 22 February 2016

Mission Profile

Definition
Identifies all of the elements that are required to define and implement a Mission Thread (MT) and to assess its performance. A mission profile is a compendium of documentation based on analysis of various resources such as mission profile templates, architectural viewpoints, Concepts of Operations (CONOPS), commonly used standards, Tactics, Techniques, and Procedures (TTPs), and Standard Operating Procedures (SOP).

Source
Coalition Interoperability Assurance and Validation (CIAV) Mission Profile Review of the Air Track Management Service of the Battlespace Management (BM) Coalition Mission Thread (CMT) and Coalition Interoperability Assurance and Validation (CIAV) Building Mission Profile Templates: Tactics, Techniques and Procedures (TTP)

See Also
Coalition Mission Thread (CMT)
Mission Thread (MT)

Mission Thread (MT)

Definition
The operational process for executing specific warfighting capabilities in order to support Command objectives. Mission threads are operationally driven, technically supported descriptions of the end-to-end interrelated activities required to execute a mission or a mission task. They are an essential part of the information management of the forces. Specifically, the Information Management of critical data from mission thread execution contributes to commander's obtaining Information Superiority and the Initiative to act within the battlespace as well as ensuring Unity of Effort among Coalition forces.

Source
Multinational Interoperability Council (MIC) Mission Thread Analysis Document

See Also
Coalition Mission Thread (CMT)
Mission Thread (MT) Services

Mission Thread (MT) Services

Definition
Capabilities and functionalities provided by applications, systems, and Systems of Systems (SoS) that are required to facilitate an MT. Mission enablers comprised of essential tasks/activities that need to be completed in order for the MT to be considered operational.

Source
Coalition Interoperability Assurance and Validation (CIAV) Building Mission Profile Templates: Tactics, Techniques and Procedures (TTP); and Mission Based Interoperability (MBI) Coalition Interoperability Assurance and Validation (CIAV) Guide to Achieving End-to-End Coalition Operational Mission Data Interoperability for Joint Inter-Agency, Inter-Governmental, and Multi-National Data Sharing

See Also
Coalition Mission Thread (CMT)
Mission Thread (MT)
Mission Profile

Mobile Device Service (MDS)

Definition
The set of services required to provide Mission Partner Environment – Information System (MPE-IS) Client capabilities on a mobile device (smartphone, tablet, etc.).

Source
Derived from: U.S. Pacific Command (PACOM) presentation to the Mission Partner Environment Executive Steering Committee (MPE ESC), 11 February 2016

See Also
Mission Partner Environment – Information System (MPE-IS) Client
Multi-Enclave Client (MEC)

Multi-Enclave Client (MEC)

Definition
An end-user device that supports multiple, technically isolated client interfaces, each of which is specific to a single mission enclave and maintains an isolated/encrypted interconnect to that mission enclave. A MEC offers users a simple, single interface to all their networks and saves on desktop surface space, floor space, power consumption, and cooling over using multiple, single enclave clients. A MEC can also have encryption built into the client. MEC is related to the industry term: Multilevel Secure Desktop.

Source
Derived from: Mission Partner Environment – Information System Reference Architecture (MPE-IS RA), Ver. 1.00, 23 March 2016

Multinational Force (MNF)

Definition
A force composed of military elements of nations who have formed an alliance or coalition for some specific purpose.

Source
Joint Publication (JP) 1-02, 15 June 2015

Multinational Information Sharing (MNIS) Program Office

Definition
The Defense Information Systems Agency (DISA) program office supporting implementation of assigned Mission Partner Environment (MPE) capabilities. The MNIS Program Office manages a portfolio of initiatives to improve interoperability and information sharing with coalition partners. It provides standard community of interest services and applications to facilitate collaboration among DoD components and foreign nations.

Source
Defense Information Systems Agency (DISA) website

Reference
https://www.disa.mil/Mission-Support/Command-and-Control/MNIS

2.13 N-Terms

National Guard Civil Support (NGCS)

Definition
Support provided by the National Guard, while in Title 32 [United States Code] duty status, to Civil Authorities, for Domestic Operations and for designated law enforcement and other activities.

Source
National Guard Regulation (NGR) 500-1

See Also
Defense Support of Civil Authorities (DSCA)

National Guard Communications Element (NGCE)

Definition
An organization consisting of deployable Command, Control, Communications and Computers (C4) capabilities tailored to the Homeland Defense/Civil Support (HD/CS) mission space and Army National Guard (ARNG) or Air National Guard (ANG) communications personnel necessary to employ the equipment. Soldiers and Airmen assigned to the NGCEs are task organized from existing National Guard (NG) units or organizations. NGCEs can rapidly respond within each state and territory, and permit NG leadership to efficiently leverage these capabilities on a regional or nationwide basis during Incidents of National Significance.

Source
National Guard Communications Element (NGCE) Mission Statement, National Guard Bureau (NGB) J6/C4

National Guard Domestic Operations (NGDO)

Definition
The training, planning, preparing, and operating of National Guard units and forces conducted in the Homeland.

Source
National Guard Regulation (NGR) 500-1

National Network Interface (NNI)

Definition
A component of the Mission Partner Gateway – Extended (MPGW-X) that serves as a gateway between two countries, generally U.S. network and another nation's networks. Its purpose is to allow one high-assurance gateway to support and provide high assurance encryption security for multiple Partner Network Interfaces (PNIs). NNI is the Joint Information Environment (JIE) connection point to a mission partner national network.

Source
Derived from: Mission Partner Gateway – Extended (MPGW-X) Service Description (SD), Version 2.2, 22 February 2016

See Also
Mission Partner Gateway – Extended (MPGW-X)
Partner Network Interface (PNI)

National Response Framework (NRF)

Definition
A guide produced by the U.S. Department of Homeland Security (DHS). The guide describes how the U.S. responds to all types of disasters and emergencies. It is built on the National Incident Management System, which aligns key roles and responsibilities to organizations across the country. The most current NRF is the Second Edition, May 2013.

Source
National Guard Bureau (NGB) Lexicon, as presented at the Senior Engineering Working Group (SEWG) Meeting on 6 August 2015 and National Response Framework (NRF), 2nd Edition, May 2013

Network Contributing Mission Partner (NCMP)

Definition
A mission partner that connects a network extension to the federation of networks established for the event.

Source
Joining, Membership, and Exiting Instructions (JMEI) v1.10, 11 August 2014

Network Interconnection Point (NIP)

Definition
The physical linkage of a Network Contributing Mission Partner (NCMP) network contribution with equipment of facilities not belonging to that network.

Source
U.S. DoD Episodic Mission Partner Environment Joining Instructions, Version 1.10, 11 August 2014

See Also
Network Contributing Mission Partner (NCMP)

Network Service Point (NSP)

Definition
The logical point between the network and transport layers where network services are delivered to the transport layer; the location of this point is identified to the network service provider by the NSP address. For the purpose of Mission Partner Environment – Information System (MPE-IS), NSPs may include the following: Multiprotocol Label Switching – Common Mission Network Transport Provider Edge (MPLS-CMNT PE) Router, MPLS-CMNT Customer Edge (CE) Router, Mission Partner Gateway – UNCLASSIFIED (MPGW-U), MPGW – SECRET (MPGW-S), and MPGW – Extended (MPGW-X).

Source
Derived from: The Open Systems Interconnection Model (See International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7498-1)

Non-Governmental Organization (NGO)

Definition
A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society.

Source
Joint Publication (JP) 1-02, 15 June 2015

Reference
http://ngos.org/what-is-an-ngo/

Non-Secure Internet Protocol Router Network (NIPRNET)

Definition
Commonly referred to as the "`Non-classified' IP Router Network," it is a DoD, private IP network used to exchange UNCLASSIFIED information, including information subject to controls on distribution.

Source
Defense Information Systems Agency (DISA) Sensitive But UNCLASSIFIED (SBU) Website

Reference
http://disa.mil/network-services/Data/SBU-IP

2.14 O-Terms

Operational Impacts (OIs)

See Capabilities/Limitations, Operational Impacts (CAPS/LIMS/OIs).

Operational Information Exchange Requirements (O-IER)

See Information Exchange Requirement (IER).

Operational Network Domain (OND)

Definition
A set of communication network resources that fall under the jurisdiction of a Joint Force Commander or Combatant Commander required by forces under the commander's Operational Control (OPCON). The purpose of the OND is to allow the commander to implement applications, sensors, and controllers; and connect to partners that involve a level of risk that may be higher or lower than that acceptable to the entire DoD enterprise. The OND provides the commander with the ability to manage risk to cyber assets, just as the commander manages risk when employing forces.

Source
Cieslak, Randall (U.S. Pacific Command (PACOM) Chief Information Officer (CIO)), "Network Design proposal for the JIE and the MPE," Version 1.1, 14 November 2013

Operational Requirements Master List (ORML)

Definition
The Coalition Interoperability Assurance and Validation (CIAV) Requirement tracking mechanism. When a requirement is validated and officially enters the U.S. CIAV process, it is added to the list and assigned a unique tracking number which follows it throughout the CIAV process. CIAV Process Phase 1 of 4.

Source
Derived from: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5128 (Draft)

See Also
Coalition Interoperability Assurance and Validation (CIAV) Request for Information (RFI)
Coalition Interoperability Assurance and Validation (CIAV) Requirement

2.15 P-Terms

Partner Network Interface (PNI)

Definition
A component of the Mission Partner Gateway – Extended (MPGW-X). PNI is the interface gateway that provides both connection and protection between a U.S. DoD network and a mission partner's network within a single Information Control Domain (ICD). PNI is a logical interface point where the U.S. portion of an enclave meets a partner nation or nations' portion of the enclave.

Source
Mission Partner Gateway – Extended (MPGW-X) Service Description (SD), Version 2.2, 22 February 2016

See Also
National Network Interface (NNI)
Mission Partner Gateway – Extended (MPGW-X)
Information Control Domain (ICD)

Pegasus

Definition
A Combined Communications Electronics Board (CCEB) initiative that will deliver significantly improved Five Eyes (Australia/Canada/New Zealand/United Kingdom/U.S.) National-to-National SECRET network connectivity to all CCEB nations. Pegasus is a framework to facilitate information sharing over SECRET Internet Protocol Router Network (SIPRNET) Releasable in the U.S. It is not a Program of Record. There are multiple service providers in the U.S. and other countries. Deliverables include: making it significantly easier to Email other CCEB nationals through the use of their native Email address, rather than having multiple unique Email addresses, as in legacy Griffin; delivering new two-way web browse services so users can access web information across all CCEB national SECRET networks; delivering new access to interconnected Secure Voice services, and delivering new desktop chat services. Capabilities are delivered in coordinated spirals. Services are managed under the Pegasus Service Operations Management (PSOM) framework.

Source
Allied Communications Publication (ACP) 230, March 2015

See Also
Coalition Network Operations Center (CNOC)/National Network Operations Center (NNOC)
Five Eyes (FVEY)

Phase 0 – V

Definition
In joint operation planning, definitive stages of an operation or campaign during which a large portion of the forces and capabilities are involved in similar or mutually-supporting activities for a common purpose. Notional Operation Plan Phases are Phase 0 – Shape, Phase I – Deter, Phase II – Seize Initiative, Phase III – Dominate, Phase IV – Stabilize, Phase V – Enable Civil Authorities.

Source
DoD Instruction (DoDI) 8110.01, 6 February 2004

2.16 R-Terms

Reconnaissance (RECON) Reporting

Definition
An application used by the State of Florida State Emergency Response Team (SERT) Reconnaissance (RECON) Unit, which operates in support of the State of Florida Division of Emergency Management. SERT is composed of county, state, federal, volunteer, and mutual aid entities. The SERT RECON unit provides an initial assessment of the impacted area boundaries, evacuation routes, and communities. SERT RECON unit personnel utilize the RECON Reporting application to provide information about their mission, findings, recommendations, and other relevant or requested information. The RECON Reporting application is a web-based system, allowing for ready access by authorized users who can connect to the Internet and application Website.

Source
State of Florida Division of Emergency Management briefing provided to the Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG) in August 2015

Red Network

Definition
Indicates the network is in a secure facility and the data is not encrypted (commonly referred to as the “plaintext” interface).

Source
Derived from: Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015

Repurposed Hardware and Software

Definition
Attendant hardware and software (workstations, routers, hard drives, servers and Command and Control (C2) systems, etc.) that can be modified to operate within a federated mission network, separate from SECRET Internet Protocol Router Network (SIPRNET), to facilitate information sharing with mission partners.

Source
Derived from: RAND Study 2013; Toward a Coalition Contingency Mission Network, Building on the Afghanistan Mission Network; pgs. 54-55 and Future Mission Network 90-day Study Report, 17 December 2012, Refer to "Third Stack”, pg. B-7.

2.17 S-Terms

Shared Services Configuration

Definition
One of the three service configurations for Mission Partner Environment – Information System (MPE-IS). This configuration provides a single application service point with all members of the mission enclave agreeing to a common set of shared application services managed by she shared service host. Shared services may be extended to disadvantaged partners, or those that do not have sufficient infrastructure to support information sharing, by the mission enclave host or one of the other enclave members.

Source
Mission Partner Environment – Information System Reference Architecture (MPE-IS RA), Ver. 1.00, 23 March 2016

Situational Awareness Geospatial Enterprise (SAGE)

Definition
Information system architecture designed to distribute and empower all U.S. Northern Command (NORTHCOM) Mission Partners (MPs) with actionable data associated with Earth's geography, locations, features, boundaries, and other topographical entities, anywhere in the world. SAGE is run by the Command and Control directorate at USNORTHCOM, Peterson Air Force Base. There are 4 major components to SAGE: (1) The Global Command and Control System (GCCS)/Geospatial Information System (GIS) architecture where geospatial analysis and data collection occurs; (2) Google Earth KML publishing, which enables GCCS tracks directly to SAGE users; (3) ArcGIS Server web services that provide industrial GIS use for Federal and State partners and provides a SAGE web map; and (4) A web front end that allows users to upload and integrate their data within SAGE.

Source
U.S. Northern Command (NORTHCOM) Situational Awareness Geospatial Enterprise (SAGE) Website

Reference
https://sageearth.northcom.mil

Software Defined Network (SDN)

Definition
Software-defined networking (SDN) is an approach to computer networking that uses abstraction to create more agile, flexible, and efficient topologies and services. The term encompasses three complimentary technologies:

- Programmable networks (SDN): separates the network management and data planes to provide centralized control of network resources for efficient provisioning and operations of network services.
- Network Function Virtualization (NFV): transforms traditional hardware based network appliances into virtual machines or services that can run in software to accelerate innovation and provisioning.
- Network Virtualization: abstracts the network used by virtual servers to create logical, virtual networks that are decoupled from the underlying network hardware.

SDN technologies can be applied across networking domains, from inside the datacenter to across the WAN, and are being used for higher level services such as load balancing and network security.

Source
Derived from: Various Industry Sources

Reference
DOD CIO SDN Working group:
https://dodcioext.osd.mil/Collaboration/SDNWorkingGroup/SitePages/Home.aspx

Stability Operations

Definition
An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe

and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.

Source
Joint Publication (JP) 3-0, 11 August 2011

State Watch Office Incident Tracker

Definition
The application used by the State of Florida Division of Emergency Management. It is a Web-based information log with mapping and notification capabilities. The State Watch Office uses it to track day-to-day incidents, share information, and track notification. Incidents are events in the state with a real or potential impact on public safety, law enforcement, or other high-visibility or high-impact considerations.

Source
State of Florida Division of Emergency Management briefing provided to the Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG) in August 2015

System Information Exchange Requirement (S-IER)

See Information Exchange Requirement (IER).

2.18 T-Terms

Tactical Processing Node (TPN)

Definition
A TPN provides services very similar to those of CDCs or IPNs but are optimized for the tactical or deployed environment. TPNs will connect to the JIE network whether in garrison or deployed, but may do so in different ways (e.g., terrestrial fiber vs. satellite connectivity).

Source
DoD Data Center Reference Architecture Version 1.10, 25 April 2014

Theater Battle Management Core System (TBMCS)

Definition
A joint program, managed by the U.S. Air Force, with U.S. Navy and U.S. Marine Corps participation. While the Army does not use the system, it has other systems that feed data to the TBMCS. It supports Air Task Order (ATO) planning and development, and provides the automated tools necessary to generate, disseminate, and execute the ATO and Air Control Order in Joint, coalition, and other contingencies.

Source
U.S. Marine Corps (USMC) Systems Development Website

Thick Client

Definition
(also called heavy, rich, or fat client) A computer (client) in client–server architecture or networks that typically provide rich functionality independent of the central server. Originally known as just a "client" or "thick client," the name is contrasted to thin client, which describes a computer heavily dependent on a server's applications.

Source
Widely used industry term

Reference
http://www.techterms.com/definition/thickclient

Thin Client

Definition
A lightweight computer that is purposely built for remoting into a server (typically desktop virtualization resources). It depends heavily on another computer (its server) to fulfill its computational roles. This is different from the traditional desktop Personal Computer (PC) (thick client), which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from hosting a shared set of virtualized applications, a shared desktop stack or virtual desktop, to data processing and file storage on the client or users behalf.

Source
Widely used industry term

Reference
http://techterms.com/definition/thinclient

Third Stack

Definition
The virtual or physical Information Technology (IT) equipment (workstations, routers, security components, servers, applications, and peripherals, etc.) necessary to establish a mission network that facilitates information sharing with mission partners. U.S. forces typically deploy with two sets of IT equipment (Non-secure Internet Protocol Router Network (NIPRNET) and SECRET Internet Protocol Router Network (SIPRNET)) for the conduct of operations. The establishment of an episodic mission enclave requires U.S. forces to possess a "third stack" of IT equipment on which to operate with Mission Partners (MPs).

Source
Derived from: Future Mission Network 90-day Study Report, 17 December 2012

Trusted Network Environment® (TNE®)

Definition
The TNE® is a certified commercial off-the-shelf Multi-Level Security technology. The TNE® is an environment implementing four major concepts supporting secure information sharing and collaboration: mathematically compared sensitivity labels; a hardened trusted operating system; unique security domain interfaces; and deep content inspection providing data sanitization and threat reduction from viruses and malware.

Note: TNE® is a registered trademark of General Dynamics Mission Systems.

Source
U.S. Battlefield Information Collection and Exploitation Systems – Extended (U.S. BICES-X) Trusted Network Environment® Technology Information Paper, November 2013

See Also
U.S. Battlefield Information Collection and Exploitation Systems – Extended (U.S. BICES-X)

Reference

http://gdmissionsystems.com/cyber/products/trusted-computing-cross-domain/trusted-network-environment-tne/

2.19 U-Terms

UNCLASSIFIED Information Sharing Service (UISS)

Definition
Provides structured (e.g., file sharing and calendaring) and unstructured (e.g., wikis, blogs, and forums) collaboration capabilities to the enterprise for the purposes of UNCLASSIFIED information sharing with multinational partners, non-governmental organizations, the various U.S. Federal and State agencies, and members of the public and private sectors. Enables effective information exchange and collaboration between the U.S. DoD and any external country, organization, agency, or individual that does not have ready access to traditional DoD systems and networks. These mission partners include, but are not limited to, U.S. government agencies; foreign governments and their militaries; International Organizations (IOs); Regional Organizations (ROs); Non-Governmental Organizations (NGOs); State, local, and tribal authorities; and members of the public and private sectors. It enables professional networking and communication, increases situational awareness, establishes pre-defined communications channels, relationships and information workflows, and provides a forum for sharing lessons learned and best practices in a wide variety of contexts including crisis response, humanitarian assistance, disaster relief, training, and exercises. UISS capabilities include: All Partners Access Network (APAN) which is a web-based, non-military collaboration platform.

Source
Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6285.01C, 15 May 2013

See Also
All Partners Access Network (APAN)

Unified Cross Domain Services Management Office (UCDSMO)

Definition
The organization responsible for centralized coordination and oversight of all cross domain activities and investments for the DoD and Intelligence Community (IC). UCDSMO functions include the support for DoD information sharing objectives by emphasizing expedited delivery to the field of Cross Domain (CD) capabilities that meet all applicable security requirements and establishing and providing CD criteria and standards.

Note: Previous name: Unified Cross Domain Management Office (UCDMO).

Source
Derived from: DoD Instruction (DoDI) 8540.01, 8 May 2015

U.S. Battlefield Information Collection and Exploitation Systems (U.S. BICES)

Definition
The U.S. national contribution to the BICES environment and is chartered with providing North Atlantic Treaty Organization (NATO) SECRET connectivity to all U.S. Combatant Commands/Services/ Agencies. Through U.S. BICES, all U.S. users can access NATO SECRET and other SECRET networks and nations via shared gateways. In addition to connectivity, U.S. BICES is the mechanism by which all U.S. producers must disseminate releasable intelligence into the BICES environment.

Source
Derived from: U.S. Battlefield Information Collection and Exploitation Systems (BICES) Service Catalog v3.0 and Under Secretary of Defense for Intelligence (USD(I)) Memorandum, 26 February 2007, Subject: Intelligence Support to North Atlantic Treaty Organization (NATO) International Security Assistance Force (ISAF) for Afghanistan

See Also
Battlefield Information Collection and Exploitation Systems (BICES)
U.S. Battlefield Information Collection and Exploitation Systems – Extended (U.S. BICES-X)

Reference
http://usbices.osd.mil/

U.S. Battlefield Information Collection and Exploitation Systems-Extended (U.S. BICES-X)

Definition
Also known as the U.S.BICES-X Enterprise. The primary resource for the dissemination of intelligence data between the U.S. Intelligence Community (IC), U.S. Combatant Commands, the DoD, U.S. government services and agencies, and Partner Nations (PNs). A PN is a country that works with the U.S. in a specific situation or operation. When there is an arrangement between two or more PNs for a common purpose, a coalition is formed.

Source
U.S. Battlefield Information Collection and Exploitation Systems - Extended (U.S. BICES-X) Enterprise Technical Data and Architecture Package, Version 2015-8.0

See Also
Battlefield Information Collection and Exploitation Systems (BICES)
U.S. Battlefield Information Collection and Exploitation Systems (U.S. BICES)

U.S. Coalition Interoperability Assurance and Validation (U.S. CIAV)

Definition
The U.S. portion of the international CIAV organization led by an O-6 level individual assigned to Defense Information Systems Agency (DISA) and with subordinate Service component elements (i.e., U.S. Army CIAV, Navy CIAV, etc.) to support the international efforts. The organization and Service components, along with Mission Partners, host the series of labs that comprise the Coalition Verification and Validation Environment (CV2E) and interface directly with the mission partners on CIAV Assurance and Validation (A&V) and Desktop Analysis (DTA) events. CIAV requirements, events, issues and concerns are addressed at quarterly CIAV Working Groups (WGs) with the international community. U.S. CIAV receives direction from the Mission Partner Environment Executive Steering Committee (MPE ESC) CIAV WG Lead.

Source
U.S. Coalition Interoperability Assurance and Validation (CIAV) Chief of Staff

See Also
Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG)
Mission Partner Environment Executive Steering Committee (MPE ESC) Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG)

2.20 V-Terms

Virtual Data Center (VDC)

Definition
A Mission Partner Environment – Information System (MPE-IS) implementation of a Software Defined Data Center that supports the rapid provisioning of mission enclaves and supporting services such that all mission enclaves configured within a VDC are isolated from each other.

The instantiation of Data Center Virtualization (DCV) technology within a physical DoD data center. The VDC virtualizes the key elements of a physical data center: processing, networking, security, and storage. Virtualizing these elements enables multiple, logically separate SECRET//Releasable (SECRET//REL) mission enclaves to be rapidly established based on varying mission operations.

Source
Derived from: Mission Partner Environment – Information System (MPE-IS) Virtual Data Center (VDC) Service Description, Version 0.8, 1 February 2016

See Also
Data Center Virtualization (DCV)

Virtual Desktop Infrastructure (VDI)

Definition
VDI is a widely used industry term referring to the process of running a user desktop inside a virtual machine that lives on a server in the datacenter. It is a powerful form of desktop virtualization because it enables fully personalized desktops for each user with all the security and simplicity of centralized management.

VDI enables customers to streamline management and costs by consolidating and centralizing the desktops while delivering end users' mobility and the freedom to access virtual desktops anytime, from anywhere, on any device. It is important to understand however, that VDI is only one form of desktop virtualization.

Source
Derived from: Multiple industry sources

Virtual Machine (VM)

Definition
A widely used industry term for a software implementation of a physical machine (for example, a computer) that executes programs like a physical machine. The end user has the same experience on a VM as they would have on dedicated hardware.

Source
Derived from: Multiple industry sources

Virtual Routing and Forwarding (VRF)

Definition
In Internet Protocol (IP)-based computer networks, VRF is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. VRF works with Multiprotocol Label Switching (MPLS) on black core networks (such as MPLS-Common

Mission Network Transport (CMNT)) to isolate the traffic from each mission enclave into its own virtual circuit allowing logical separation of traffic based on classification.

Source
Derived from: Yee, Garrett, Colonel, U.S. Army, "A Black Core Network Primer," Army Communicator 2012 and multiple industry sources

2.21 Z-Terms

Virtual Secure Enclave (VSE)

Definition
Virtual Security Enclaves (VSEs) are network enclaves logically separated from underlying physical network transport via encrypted Virtual Private Network (VPN) layer(s) with controlled data flow between network enclaves via policy enforced Controlled Interfaces. These enclaves are created within DoD networks and are configured with layered defenses creating internal boundaries which act as cyber fortifications, blocking and delaying attackers in the event they are able to penetrate external defenses.

Source
System Design Description (SDD) For Virtual Secure Enclave (VSE), 13 Mar 2015, Department of the Navy Space and Naval Warfare Systems Center, Pacific (SSC Pacific)

Voice and Video Cross-Domain Solution (V2CDS)

Definition
V2CDS is a transfer/multi-level solution that delivers secure, real-time Voice over Internet Protocol (VoIP) communication and conferencing with point-to-point video capability across multiple security domains.

Source
Voice and Video CDS v1.0.2 (240-373-0796), 29 March 2016, Unified Cross Domain Services Management Office (UCDSMO)

Zero Client

Definition
A widely used industry term (also known as ultrathin client) for a server-based computing model in which the end user's computing device has no local storage. A zero client can be contrasted with a thin client, which retains the operating system and each device's specific configuration settings in flash memory.

Source
Derived from: Multiple industry sources

Appendix A List of Acronyms

Acronym	Description
A&V	Assurance and Validation
AMN	Afghanistan Mission Network
ANG	Air National Guard
AOR	Area of Responsibility
APAN	All Partners Access Network
APIIN	Asia-Pacific Intelligence Information Network
ARNG	Army National Guard
ASP	Application Service Points
AVE	Agile Virtual Enclave
BICES	Battlefield Information Collection and Exploitation Systems
C2	Command and Control
C5ISR	Coalition Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAPS/LIMS	Capabilities and Limitations
CDC	Core Data Center
CDCE	Cross Domain Controlled Environment
CDCG	Cross Domain Controlled Gateway
CDS	Cross Domain Solution
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFBLNet	Combined Federated Battle Laboratories Network
CIAV	Coalition Interoperability Assurance and Validation
CIO	Chief Information Officer
CMFC	Combined Maritime Forces Central
CMFP	Cooperative Maritime Forces Pacific
CMNT	Common Mission Network Transport
CMT	Coalition Mission Thread
CNOC	Coalition Network Operations Center
COI	Community of Interest
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operational Picture
COTS	Commercial-Off-The-Shelf
CPN	CENTCOM Partner Network
CSfC	Commercial Solutions for Classified
CTTP	Coalition Tactics, Techniques, and Procedures

Acronym	Description
DCO	Defensive Cyberspace Operations
DCV	Data Center Virtualization
DIL	Disconnected, Intermittent, and/or Limited bandwidth
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD CIO	Department of Defense Chief Information Officer
DoDIN	DoD Information Network
DOMS	Director Of Military Support
DOMOPS	Domestic Operations
DSCA	Defense Support of Civil Authorities
DTA	Desktop Analysis
ECDS	Enterprise Cross Domain Service
Email	Electronic Mail
ESC	Executive Steering Committee
FBI	Federal Bureau of Investigation
FDR	Foreign Disaster Relief
FHA	Foreign Humanitarian Assistance
FMN	Federated Mission Networking
FMV	Full Motion Video
FTI	Federated TNE® Infrastructure
FVEY	Five Eyes (U.S., United Kingdom, Australia, Canada, New Zealand)
GATOR	Geospatial Assessment Tool for Operations and Response
GCCS	Global Command and Control System
GGC	Global Gray Core
GIEEP	Geospatial Information Interoperability Exploitation Portable
GW	Gateway
HA/DR	Humanitarian Assistance/Disaster Relief
HACI	High Assurance Controlled Interface
HAIPE	High Assurance Internet Protocol Encryptor
HD	Homeland Defense
HD/CS	Homeland Defense/Civil Support
HDA	Homeland Defense Activity
HSIN	Homeland Security Information Network
IAP	Internet Access Point
ICD	Information Control Domain
IDT	Integrated Design Team

Acronym	Description
IPN	Installation Processing Node
IPT-PE	Internet Protocol Transport – Provider Edge
ISAF	International Security Assistance Force
IT	Information Technology
JIE	Joint Information Environment
JMEI	Joining, Membership, and Exiting Instructions
JRSS	Joint Regional Security Stack
JTSO	JIE Technical Synchronization Office
LEO-EP	Law Enforcement Online - Enterprise Portal
MEC	Multi-Enclave Client
MNIS	Multinational Information Sharing
MP	Mission Partner
MPE	Mission Partner Environment
MPE-IS	Mission Partner Environment – Information System
MPE-IS ESC	Mission Partner Environment – Information System Executive Steering Committee
MPGW	Mission Partner Gateway
MPGW-S	Mission Partner Gateway - SECRET
MPGW-U	Mission Partner Gateway - UNCLASSIFIED
MPGW-X	Mission Partner Gateway - Extended
MT	Mission Thread
NATO	North Atlantic Treaty Organization
NCMP	Network Contributing Mission Partner
NG	National Guard
NGB	National Guard Bureau
NGCE	National Guard Communication Element
NGCS	National Guard Civil Support
NGDO	National Guard Domestic Operations
NGO	Non-governmental Organization
NIPRNET	Non-Secure Internet Protocol Router Network
NNI	National Network Interface
NNOC	National Network Operations Center
NNT	Network Normalization and Transport
NSA	National Security Agency
OND	Operational Network Domain
ORML	Operational Requirements Master List
PNI	Partner Network Interface

Acronym	Description
RECON	Reconnaissance
RFI	Request for Information
SAGE	Situational Awareness Geospatial Enterprise
SBU	Sensitive But UNCLASSIFIED
SD	Service Description
SDN	Software Defined Network
SEWG	Senior Engineering Working Group
SERT	State Emergency Response Team
SIPRNET	Secret Internet Protocol Router Network
SOP	Standard Operating Procedure
TBMCS	Theater Battle Management Core System
TCN	Tactical Communications Node
TNE®	Trusted Network Environment
TPN	Tactical Processing Node
TTP	Tactics, Techniques, and Procedures
UC	Unified Capabilities
UCDSMO	Unified Cross Domain Services Management Office
UISS	UNCLASSIFIED Information Sharing Service
U.S. BICES	U.S. Battlefield Information Collection and Exploitation Systems
U.S. BICES-X	U.S. Battlefield Information Collection and Exploitation Systems-Extended
V2CDS	Voice and Video Cross Domain Solution
VDC	Virtual Data Center
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VSE	Virtual Security Enclave
VTC	Video Teleconferencing
WAN	Wide Area Network
WG	Working Group

Appendix B References

(a) Allied Communications Publication (ACP) 122(G), February 2015, Information Assurance for Allied Communications and Information Systems

(b) Allied Communications Publication (ACP) 200(D), Vol. 2, March 2015, Maritime and Mobile Tactical Wide Area Network (MTWAN) in the Maritime Environment

(c) Allied Communications Publication (ACP) 230, March 2015, Pegasus Service Operations Management (PSOM),

(d) APAN Website, www.apan.org

(e) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5128.01, 1 October 2014, Mission Partner Environment Executive Steering Committee governance and Management

(f) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01F, 21 March 2012, Net Ready Key Performance Parameter (NR KPP)

(g) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6285.01C, 15 May 2013, Multinational and Other Mission Partner (MNMP) Information Sharing Requirements Management Process

(h) Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5128 (Draft), Mission Partner Environment Executive Steering Committee (MPE ESC) Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG) Manual

(i) Cieslak, Randall (U.S. Pacific Command (PACOM) Chief Information Officer (CIO)), “Network Design proposal for the JIE and the MPE,” Version 1.1, 14 November 2013

(j) Coalition Interoperability Assurance and Validation (CIAV) 101 Brief

(k) Coalition Interoperability Assurance and Validation (CIAV) Building Mission Profile Templates: Tactics, Techniques and Procedures (TTP)

(l) Coalition Interoperability Assurance and Validation (CIAV) Mission Profile Review of the Air Track Management Service of the Battlespace Management (BM) Coalition Mission Thread (CMT)

(m) Coalition Interoperability Assurance and Validation (CIAV) Mission Profiles Implementation Strategy

(n) Coalition Interoperability Assurance and Validation (CIAV) Mission Thread Anatomy

(o) Coalition Interoperability Assurance and Validation (CIAV) Request for Information (RFI) Standard Operating Procedure (SOP)

(p) Coalition Interoperability Assurance and Validation (CIAV) Working Group (WG) Calling Notice

(q) Coalition Mission Threads and Their Associated Services for the Mission Partner Environment (MPE) and Federated Mission Network (FMN)

(r) Committee on National Security Systems Instruction (CNSSI) No. 4009, 6 April 2015, National Information Assurance (IA) Glossary

(s) Committee on National Security Systems Policy (CNSSP) No. 19, 10 June 2013, National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products

(t) Cox, James. (December 2012). "Canada and the Five Eyes Intelligence Community," Canadian Defense and Foreign Affairs Institute

(u) Dakis, Ann. (July–September 2011). "CENTRIXS-Maritime: connecting the warfighter", CHIPS (United States Department of the Navy Chief Information Officer) XXIX (III): 54–55, ISSN 1047-9988, OCLC 6062228.

(v) Defense Information Systems Agency (DISA) Common Mission Network Transport (CMNT) website, http://www.disa.mil/Network-Services/VPN/CMNT

(w) Defense Information Systems Agency (DISA) ID32 Cross Domain Enterprise Service (CDES)

(x) Defense Information Systems Agency (DISA) Joint Regional Security Stacks (JRSS) Website, http://www.disa.mil/Initiatives/JRSS

(y) Defense Information Systems Agency (DISA) Sensitive But UNCLASSIFIED (SBU) Website, http://disa.mil/network-services/Data/SBU-IP

(z) Defense Information Systems Agency (DISA) Website, https://www.disa.mil/Mission-Support/Command-and-Control/MNIS

(aa) Department of Homeland Security’s Homeland Security Information Network (HSIN) website, https://www.dhs.gov/homeland-security-information-network-hsin

(bb) DoD Architecture Framework (DoDAF) SV-6

(cc) DoD Cybersecurity Reference Architecture (CS RA) Version 3.0 (FINAL), 24 September 2014

(dd) DoD Information Sharing Strategy, 4 May 2007

(ee) DoD Instruction (DoDI) 8110.01, 6 February 2004, Multinational Information Sharing Networks Implementation

(ff) DoD Instruction (DoDI) 8330.01, 21 May 2014, Interoperability of Information Technology (IT), Including National Security Systems (NSS)

(gg) DoD Instruction (DoDI) 8500.01, 14 March 2014, Cybersecurity

(hh) DoD Instruction (DoDI) 8540.01, 8 May 2015, Cross Domain (CD) Policy

(ii) Federal Bureau of Investigation (FBI) Law Enforcement Online – Enterprise Portal (LEO-EP) Website: https://www.cjis.gov/CJISEAI/EAIController

(jj) Future Mission Network 90-day Study Report, 17 December 2012

(kk) General Dynamics Website, Trusted Network Environment®, http://gdmissionsystems.com/cyber/products/trusted-computing-cross-domain/trusted-network-environment-tne/

(ll) Joining, Membership, and Exiting Instructions (JMEI) v1.10, 11 August 2014

(mm) Joint Information Environment (JIE) Executive Committee (EXCOM) briefing: “DoD IT Effectiveness - Building the Joint Information Environment to Enable Full Spectrum Dominance,” 18 July 2012

(nn) Joint Information Environment (JIE) Network Normalization and Transport (NNT) Integrated Design Team (IDT) Wide Area Network (WAN) Solution Architecture

(oo) Joint Information Environment (JIE) Unified Capabilities (UC) Solution Architecture

(pp) Joint Publication (JP) 1-02, 15 June 2015, DoD Dictionary of Military and Associated Terms

(qq) Joint Publication (JP) 3-0, 11 August 2011, Joint Operations

(rr) Joint Publication (JP) 3-12, 5 February 2013, Cyberspace Operations

(ss) Joint Publication (JP) 3-28, Defense Support of Civil Authorities (DSCA), 31 July 2013

(tt) Joint Publication (JP) 3-29, 3 January 2014, Foreign Humanitarian Assistance

(uu) Joint Publications (JP): https://jdeis.js.mil/jdeis/index.jsp?pindex=43

(vv) Military Standard (MIL-STD) 6016E, 20 July 2012, Tactical Data Link (TDL) 16 Message Standard

(ww) Military Standard (MIL-STD) 6017C, 31 May 2012, Variable Message Format (VMF)

(xx) Mission Based Interoperability (MBI) Coalition Interoperability Assurance and Validation (CIAV) Guide to Achieving End-to-End Coalition Operational Mission Data Interoperability for Joint Inter-Agency, Inter-Governmental, and Multi-National Data Sharing

(yy) Mission Partner Environment – Information System (MPE-IS) Global Gray Core (GGC) Service Description, Version 0.4, 29 January 2016

(zz) Mission Partner Environment – Information System Reference Architecture (MPE-IS RA), Ver. 1.00, 23 March 2016

(aaa) Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG)

(bbb) Mission Partner Environment – Information System (MPE-IS) Virtual Data Center (VDC) Service Description, Version 0.8, 1 February 2016

(ccc) Mission Partner Gateway – Extended (MPGW-X) Service Description (SD), Version 2.2, 22 February 2016

(ddd) Multinational Information Sharing (MNIS) Program Management Office (PMO) Systems Engineering Plan (SEP), 26 June 2014

(eee) Multinational Interoperability Council (MIC) Mission Thread Analysis Document

(fff) National Guard Bureau (NGB) Lexicon, as presented at the Senior Engineering Working Group (SEWG) Meeting on 6 August 2015

(ggg) National Guard Communications Element (NGCE) Mission Statement, National Guard Bureau (NGB) J6/C4

(hhh) National Guard Regulation (NGR) 500-1

(iii) National Response Framework (NRF), 2nd Edition, May 2013

(jjj) National Security Agency (NSA) Commercial Solutions for Classified (CSfC) Website: https://www.nsa.gov/ia/programs/csfc_program/

(kkk) National Security Agency (NSA) Information Assurance Directorate (IAD) Commercial Solutions for Classified (CSfC) Capability Package, 2015

(lll) Non-Governmental Organization (NGO) Website: http://ngos.org/what-is-an-ngo/

(mmm) North Atlantic Treaty Organization (NATO) Federated Mission Networking Implementation Plan, Volume I, 11 August 2014

(nnn) RAND Study 2013; Toward a Coalition Contingency Mission Network, Building on the Afghanistan Mission Network; pgs. 54-55

(ooo) State of Florida Division of Emergency Management briefing provided to the Mission Partner Environment – Information System (MPE-IS) Senior Engineering Working Group (SEWG) in August 2015

(ppp) Tech Terms Website (for widely used industry terms): http://www.techterms.com/

(qqq) The Open Systems Interconnection Model (See International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7498-1)

(rrr) The Next Wave, Volume 18, Number 4, 2011, The Security Impact of System Virtualization

(sss) Title 32, U.S. Code, Section 901

(ttt) Under Secretary of Defense for Intelligence (USD(I)) Memorandum, 26 February 2007, Subject: Intelligence Support to North Atlantic Treaty Organization (NATO) International Security Assistance Force (ISAF) for Afghanistan

(uuu) U.S. Battlefield Information Collection and Exploitation Systems - Extended (U.S. BICES-X) Enterprise Technical Data and Architecture Package, Version 2015-5.0

(vvv) U.S. Battlefield Information Collection and Exploitation Systems – Extended (U.S. BICES-X) Trusted Network Environment® Technology Information Paper, November 2013

(www) U.S. Battlefield Information Collection and Exploitation Systems (U.S. BICES) Service Catalog v3.0, Battlefield Information Collection and Exploitation Systems (BICES) 2014 Service Catalogue

(xxx) U.S. Battlefield Information Collection and Exploitation Systems (U.S. BICES) Website: http://usbices.osd.mil/

(yyy) U.S. Coalition Interoperability Assurance and Validation (CIAV) Chief of Staff

(zzz) U.S. DoD Episodic Mission Partner Environment Joining Instructions, Version 1.10, 11 August 2014

(aaaa) U.S. Marine Corps (USMC) Systems Development Website

(bbbb) U.S. Northern Command (NORTHCOM) Situational Awareness Geospatial Enterprise (SAGE) Website , https://sageearth.northcom.mil

(cccc) U.S. Pacific Command (PACOM) presentation to the Mission Partner Environment Executive Steering Committee (MPE ESC), 11 February 2016

(dddd) Using Coalition Interoperability Assurance and Validation (CIAV) to Achieve Mission-Based Interoperability, 2 December 2013

(eeee) Yee, Garrett, Colonel, U.S. Army, “A Black Core Network Primer,” Army Communicator 2012