CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-2
DISTRIBUTION: A, B, C, S

CJCSI 3340.02B
24 October 2013

JOINT ENTERPRISE INTEGRATION OF WARFIGHTER INTELLIGENCE

Reference(s): See Enclosure C.

1. Purpose. This instruction establishes policy and procedures to improve the integration of warfighter intelligence data across the Intelligence Community (IC).

a. The goal of joint enterprise integration (JEI) is the universal application of a common framework of interoperability standards for information processing networks, systems, applications, and databases at the Combatant Commands (CCMDs), Services, and Department of Defense (DoD) Intelligence Agencies. This common framework is intended to allow authorized users at all levels seamless access to and utility of data pertaining to their particular mission areas.

b. JEI is the set of processes and actions undertaken to synchronize, correlate, and deliver national security community data across intelligence enterprise architectures, enabling responsive access, configuration, manipulation, and employment of operational systems benefiting the execution of the National Military Strategy.

c. Integrating warfighter intelligence data improves users' production, analysis, and dissemination capabilities. JEI requires access (including discovery, search, retrieval, and display) to intelligence data among the warfighters, and other producers and users via standardized services and architectures. These users include, but are not limited to, the CCMDs, Services, Defense Agencies, the IC, and key partner and coalition nations.

2. Superseded/Cancellation. CJCSI 3340.02A, 16 November 2008, "Horizontal Integration of Warfighter Intelligence," is hereby superseded.

3. Applicability. This instruction applies to:

a. The CCMDs, Services (including the Service Intelligence Centers), Joint Task Forces, and the Joint Staff (JS).

b. The collection, processing and exploitation, analysis and production, and dissemination activities conducted or governed by DoD Intelligence Agencies. The DoD Intelligence Agencies are the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Security Agency/Central Security Service (NSA/CSS), and the National Reconnaissance Office (NRO).

c. Warfighter intelligence is defined as intelligence and counterintelligence (CI) data collected using multiple domains and collection disciplines at the strategic, operational, and tactical levels, and the products resulting from analysis and fusion of collected intelligence data.

4. Policy. See Enclosure A.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Summary of Changes.

a. Updated the name of the Instruction and clarified and simplified the definition.

b. Updated the document to reflect disestablishment of Joint Forces Command and the Defense Intelligence Operations Coordination Center with reassignment of responsibilities to the JS, Director of Intelligence (J-2).

c. Added a requirement for the JS J-2 to annually prioritize, track, document, and report unresolved interoperability challenges to the Vice Chairman of the Joint Chiefs of Staff (VCJCS).

d. Included the Joint Intelligence Capabilities, Assessments, and Requirements System (JICARS) concept.

e. Added a requirement to the JS J-2 to biennially publish a strategic roadmap for joint systems integration.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DoD components (to include the CCMDs), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

DAVID L. GOLDFEIN, Lt Gen, USAF
Director, Joint Staff

Enclosures:

A--Policy
B--Responsibilities
C--References
GL--Glossary

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, C, S plus the following addressees:

	Copies
Under Secretary of Defense for Acquisition, Technology, and Logistics	2
Under Secretary of Defense for Intelligence	2
Department of Defense Chief Information Officer	2
Director, Program Analysis and Evaluation	2
Director, National Reconnaissance Office	2
Director of National Intelligence	2

The Office of Primary Responsibility for the subject directive has chosen electronic distribution to the above organizations via e-mail. The Joint Staff Information Management Division has responsibility for publishing the subject directive to the SIPR Joint Electronic Library web site.

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY

1. United States Statute, IC and DoD policy, standing Executive Order, and other DoD principles direct that broad access to collected intelligence shall be provided using an integrated approach that ensures an uninhibited flow of information from all sources and databases, as authorized by appropriate clearance, mission requirement, and need to know.

2. Joint doctrine states that joint forces continually have access to national intelligence capabilities to improve in-theater analysis and production processes. A more comprehensive level of enterprise integration is required to provide this continual access to not only relevant national intelligence, but also many forms of amplifying data and concurrently produced general military intelligence.

3. To improve JEI of warfighter and national intelligence data, intelligence activities must implement best practices of data sharing among intelligence capabilities, processes, personnel, and intelligence service organizations. This improvement in JEI leverages an approach of data integration in accordance with DoD/Director of National Intelligence (DNI) directives that is streamlined and efficient within fiscal constraints, while consistent with applicable security policies.

4. Defense intelligence components shall ensure common community-wide services, applications, security, and standards are applied within the organization and across network, mission, and organizational boundaries. This strategy incorporates intelligence cross-domain architectures of the CCMDs, Services, DoD Intelligence Agencies, supporting Regional Service Centers, DoD, and key mission partners and coalition nations.

a. In order to facilitate the cross flow of intelligence information and data to operational users, CCMD Joint Intelligence Operations Centers (JIOCs), Service intelligence producers , and DoD Intelligence Agency producers shall publish intelligence data/information (including socio-cultural information) that are accessible and discoverable using compatible formats across the DoD and IC intelligence and information environments.

b. To the widest extent possible, intelligence data are accessible irrespective of the system or application that processed or exploited the intelligence data. Identity control and access management, role-based access control, and attribute-based access control means should be employed appropriate to the lowest applicable classification level of the data to allow universal access and data sharing between intelligence and command and control (C2) systems by DoD, IC, and Allied and Coalition personnel with clearance and need to know.

c. Depending on operational requirements and foreign disclosure policy, intelligence information and data are marked to support the release to appropriate coalition partners, while enabling access to coalition-derived intelligence information in a standard format.

5. Sensor data are made accessible using repeatable, standardized processes and enterprise architectures, including tagging of the data for discovery. The standard for discovery tagging is the DoD Discovery Metadata Specification (DDMS). Organizations accessing intelligence information invoke discovery processes to locate and access the data using standards-based services. To ensure integration of data, organizations conducting processing, exploitation, analysis, and production activities use standard, repeatable processes, and methods of composition through standards-based services.

6. The JS J-2 JICARS process supports community-wide ongoing integration and data compatibility efforts through a JEI requirement and assessment approach. The JS J-2 uses the JICARS process, as a collaborative environment for the CCMDs, Services, and DoD Intelligence Agencies to develop capabilities to migrate the current intelligence data environment and associated architectures toward a common framework supportive of intelligence information technology (IT) operations. These ongoing integration and data compatibility efforts include attaining the ability to access and integrate intelligence information (to include socio-cultural information) from key mission partners and coalition nations. (See Enclosure B, Responsibilities.)

7. The CCMDs, Services, and DoD Intelligence Agencies establish a seamless data sharing architecture in accordance with IC Directives, reference z, Executive Orders, Chairman Joint Chief of Staff (CJCS) Instructions and Manuals, IC Information Technology Enterprise (IC ITE) and Joint Information Environment (JIE) standards, and applicable directives.

8. The DoD Intelligence Agencies' establishment of national repositories for long-term, large-volume storage of warfighter intelligence data supports discoverability and accessibility by users other than the CCMDs and JIOCs. Commands and Services move data to these shared spaces based on pre-defined rules and within operational constraints, the limitations of system capacity (e.g., systems used for a commander's situational awareness that inherently lack memory and relay capability), and dissemination control measures.

9. The Services and DoD Intelligence Agencies shall develop publishing mechanisms compliant with service-orientated architecture cross-database

search and retrieval standards to enable federated access and discovery at the closest operationally feasible point using intelligence and C2 systems. This capability promotes joint forces data integration and systems interoperability with present IC and future mission partners.

10. Reference w requests Services and IC functional leads implement net-centric data sharing, including creating associated discovery metadata and catalogue posting to enable querying. All capabilities producing intelligence data shall data tag information at the closest operationally feasible point, to enable common utilization prior to and during analysis.

11. Future joint intelligence architectures shall incorporate CCMD and Service enterprises, DoD Intelligence Agency, and Joint Reserve Intelligence Center (JRIC) capabilities, and key mission partners and coalition nations.

12. CCMDs, Services, and DoD Intelligence Agencies maximize the use of approved multi-level security capabilities to:

a. Provide for efficient transfer of data and information across domains eliminating inefficient and non-secure methods.

b. Improve efficiency and effectiveness of automated tear line release.

c. Support data aggregation needed for advanced analytics and fusion.

d. Eliminate unnecessary data duplication.

e. Improve adaptability of data sources to new dissemination requirements.

f. Enforce mandatory access control measures based on identity and privilege.

g. Provide Coalition partners and key Allies with access to appropriate intelligence data.

13. Continuing development of Service and Joint intelligence IT architectures shall conform to established DoD governance principles of intelligence sharing. Identified governance structures shall collaborate to gather, consolidate, review, validate, and prioritize user data sharing gaps and requirements, and to support DoD, IC, and national policy guidance for joint integration efforts. Governance structures and integration efforts include, but are not limited to the Battlespace Awareness Functional Capabilities Board (BA FCB), Command, Control, Communications, and Computer/Cyber (C4/Cyber) FCB, and other FCBs, as appropriate.

(1) Joint Intelligence Capabilities, Assessments, and Requirements System (JICARS). JICARS participants include:

(a) The Service Distributed Common Ground/Surface System (DCGS) Enterprise operational users and subordinate structures.

(b) The CCMD JIOC operational users and subordinate structures.

(c) Intelligence Support Command and Control, and subordinate structures.

(d) The Joint Information Sharing Forum (JISF) (i.e. requirements, capabilities, and synchronization).

(e) ENTERPRISE RESOLVE (ER) (i.e. assessments).

(2) An integral function of continued joint and coalition architecture development is a rigorous assessment and evaluation program using JICARS processes to determine the applicability of proposed solutions to Joint Requirements Oversight Council (JROC) validated requirements, uncover performance shortfalls, and to highlight redundancies. This is especially important in addressing cross-community issues, such as between the IC and the operational organizations and forces using intelligence to effect mission accomplishment on behalf of the Joint or Coalition commander. Utilizing the lessons learned from interoperability events, Service testing, and DoD Intelligence Agency Intelligence, Surveillance, and Reconnaissance (ISR) capability assessments assist in detecting, developing, and resolving systems interoperability and data integration challenges.

14. Adherence to IT standards at the closest operationally feasible point as determined by appropriate governance bodies is critical to JEI of warfighter intelligence data. CCMD, Service, and DoD Intelligence Agency participation in the standards development process is essential to a productive capabilities development environment and an integrated and interoperable intelligence enterprise.

15. Operational intelligence IT integration of new standards and processes is achieved through the support of joint training for the CCMDs, Services, and Agencies. The JS J-2 and DIA will work with JS J7, the CCMDs, the Services, and Agencies to identify joint exercises and training events to incorporate new standards and processes with sufficient time for the training audiences to practice these standards. J-2 operational intelligence IT processes and J7 Joint Training System processes enhance the integration successes across both communities of interest (COI).

16. Thorough coordination of proposed data standards among organizations through a COI approach is necessary to ensure baseline data integration and to reduce fiscal impacts during implementation.

17. This instruction does not usurp or negate the authorities granted by law or Executive Order to the heads of the Military Services, DoD Intelligence Agencies, or other government entities.

(INTENTIONALLY BLANK)

ENCLOSURE B

RESPONSIBILITIES

1. Joint Staff, Director of Intelligence (J-2) will:

a. Assesses compliance with this instruction and policy through the Warfighter Support and Integration business practices, FCB requirements and assessment processes, and the Joint Military Intelligence Requirements Certification process.

b. Serves as the Joint Warfighter Intelligence Integration (JWII) Manager responsible for the analysis of CCMD and Military Service intelligence information integration requirements and the synchronization of related capabilities across three major intelligence systems: DCGS; JIOC; and Global Command and Control System - Integrated Imagery and Intelligence (GCCS-I3). Recommendations based on this analysis are provided to the BA FCB, C4/Cyber FCB, or other FCBs, as appropriate.

(1) Develops, manages, coordinates, collaborates, and analyzes JROC approved requirements, vets the derived JWII needs and advocates for standardization and integration of common solutions to resolve identified intelligence sharing capability gaps.

(2) Coordinates, manages, and advocates for standardization and consolidation of comparable Joint Capabilities utilized within the Joint community; advocates for integration of common solutions within the strategic DoD and IC intelligence support systems.

(3) Manages, conducts, and facilitates the JISF process to develop, coordinate, analyze, and assess JWII needs and capabilities to resolve DCGS, JIOC, and GCCS-I3 intelligence operations IT gaps, interoperability, and shortfalls. Provides a forum to foster and enable interoperability between ISR and C2 program managers, and advocates and evaluates interdependencies for net-centric data sharing.

(4) Develops, organizes, manages, and conducts ER Operational Assessments of established JWII needs and potential solutions for the DoD and IC.

(5) In coordination with DIA, facilitates identification and management of CCMD and Service operational user needs and related intelligence sharing capability gaps and advocates for common solutions.

(6) Monitors joint capability integration across the enterprise(s) for final requirements resolution.

(7) Ensures synchronization of intelligence systems requirements, functions, and capabilities with the Joint Staff J-6/Chief Information Officer-related IT portfolio efforts to enable joint interoperability of components within the DoD Information Network.

c. Advocates for JWII needs in appropriate DoD and IC governance forums and resource processes.

d. Adjudicates conflicts and identifies authoritative sources in established directives and policies.

e. Provides operational user IT expertise to standards, technical and COI working groups, forums, and governance bodies.

f. Adjudicates operational constraints on access to warfighter intelligence data between CCMDs and DoD Intelligence Agencies.

g. Employs the policies and implementation of information sharing initiatives and objectives as outlined in the DoD Information Sharing Strategy, associated Implementation Plan, and reference z in support of JEI of warfighter intelligence with present and future mission partners.

h. In conjunction with DIA, employs methods to assess the efficiency of JWII support to operational objectives and recommends changes to address identified shortfalls.

i. Conducts joint intelligence concept research, development, and assessments to identify future capabilities that enhance and enable data repositories and the JWII data.

j. Develops and produces supporting documentation.

(1) Annually assesses the success of information sharing and JIE initiatives between the CCMDs/JIOCs, DoD Intelligence Agencies, Reserve Components, and appropriate partner and coalition nations. Provides recommendations to maximize JEI among and between DoD and IC agencies and entities via the CJCS and Under Secretary of Defense for Intelligence to the Secretary of Defense (or designated representatives), and the DNI for action.

(2) Develops and publishes a biennial strategic roadmap for joint operational intelligence IT integration outlining a defined end state for CCMD, cross-Service, supporting DoD Agencies, and coalition warfighter-intelligence

operational IT architectures and information sharing, to include performance milestones and appointed offices of primary responsibility.

(3) Prioritizes and tracks unresolved intelligence operations IT integration challenges impacting the DoD in an annual report to the VCJCS. Identifies the critical challenges and provides a status update on courses of action taken and estimated time to problem resolution.

k. Advocates for operational intelligence IT integration of intelligence standards and processes into joint training. Collaborates with CCMDs, Services, Agencies, and coalition and partner nations on the integration of new processes and standards in joint exercises.

2. Director, Defense Intelligence Agency (DIA) will:

a. Develops and manages those Military Intelligence resources and capabilities under the purview of the DIA that fall under the Military Intelligence Program, and the National Intelligence Program.

b. Provides JIOC IT infrastructure. Works with service providers and functional managers to ensure integration of validated capabilities.

c. Develops and implements a systems architecture and JWII plan for the CCMDs (J-2/JIOC) and associated JRICs consistent with Defense Intelligence Information Enterprise, DoD, and the Office of the Director of National Intelligence (ODNI) information sharing environment initiatives, including cross-domain/cross-security capabilities.

d. Facilitates access to DoD Intelligence Agencies' databases for the CCMDs/JIOCs, and serves as the DoD conduit for interagency IT connectivity and interoperability. Where possible, facilitates information and/or data access for key partner and coalition nations.

e. Coordinates with the Joint Staff on all CCMD IT requirements and resolution thereof.

f. Provides functional expertise to IT standards working groups, technical working groups, and other COI.

g. Facilitates DIA-proposed JWII needs submission for JICARS/JISF consideration.

3. Directors of the DoD Intelligence Agencies will:

a. Oversee emerging capabilities compliancy with enterprise and standards-based services for access to data, and adherence to COI-developed agreements, and to standards-based, approved interfaces with other shared environments.

b. Operate and manage national repositories of warfighter intelligence data inaccessible to users outside their normal operational environment (e.g., Theater).

c. Assist CCMDs in developing procedures for tagging data with discovery metadata and making data from national repositories accessible using standards-based services.

d. Employ rule sets and standards for inclusion in all appropriate Joint Capabilities Integration and Development System documents to maximize data sharing and usability.

e. Provide functional expertise to IT standards working groups, technical working groups, and COI, as required.

f. Develop and advocate enterprise and standards-based approaches to system interoperability and data integration with present and future mission partners in support of the CCMDs (J-2/JIOCs) and Services. Uses COI approaches to gain agreement on vocabularies.

g. Develop and maintain education, training, and exercises required to implement JWII policy and procedures.

h. Facilitate DoD Intelligence Agency proposed enterprise needs submission for JICARS/JISF consideration.

4. Chiefs of the Military Services will:

a. Oversee emerging capabilities compliancy with enterprise and standards-based services for access to data, and adherence to COI-developed agreements, and to standards-based, approved interfaces with other shared environments.

b. Provide functional expertise to IT standards working groups, technical working groups, and COI.

c. Develop and maintain education and training required to implement JWII policies and procedures.

d. Evaluate and recommend best JWII processes and/or procedures for incorporation into the intelligence COI to the Joint Staff and Office of the Undersecretary of Defense for Intelligence.

e. Facilitate Service proposed enterprise needs submission for JICARS/JISF consideration.

5. Combatant Commanders will:

a. Store warfighter intelligence data at discoverable and accessible locations and tag the information with discovery metadata at either the source or the closest operationally and technically feasible point.

b. Host JWII architecture components of national repositories, as required.

c. Develop knowledge management procedures for tagging data with discovery metadata, and for posting data to national repositories. For each type of data, coordinate with the authoritative DoD Intelligence Agency to produce business rules to:

(1) Identify data that remains inaccessible and undiscoverable.

(2) Establish time requirements for tagging and posting data.

(3) Determine the authoritative data source(s).

(4) Mitigate operational constraints (e.g., bandwidth, guard capacity) and dissemination control measures (e.g., originator controlled above the tear line).

d. Participate in appropriate governance processes, and advocate for operational needs in conjunction with the JS J-2.

e. Develop and maintain education and training required to implement JWII policies and procedures.

f. Facilitate CCMD proposed enterprise needs submission for JICARS/JISF consideration.

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

a. Under-Secretary of Defense for Intelligence, 2010, “Defense Intelligence Strategy”

b. JROC Memorandum 124-04, 9 July 2004, “Common Data Standards and Format to Enable Horizontal Integration (HI)”

SUPPLEMENTAL DOCUMENTATION

CJCS EXORD, Modification 3, Joint Intelligence Operations Center (JIOC), 040001Z October 2011

CJCSI 3170.01 Series, “Joint Capabilities Integration and Development System”

CJCSI 3265.01 Series, “Command and Control Governance Management”

CJCSI 3312.01 Series, “Joint Military Intelligence Requirements Certification”

CJCSI 5123.01 Series, “Charter of the Joint Requirements Oversight Council”

CJCSI 6211.02 Series, “Defense Information System Network (DISN): Responsibilities”

CJCSI 6212.01 Series, “Net Ready Key Performance Parameter (NR KPP)”

Committee on National Security Systems (CNSS) Instruction No. 4009, June 2006, “National Information Assurance (IA) Glossary”

DCID 6/6, 30 June 1998, “Security Controls on the Dissemination of Intelligence Information”

Director of National Intelligence and Undersecretary of Defense for Intelligence, 2013, “Consolidated Intelligence Guidance”

DoDAF Version 2.0, 28 May 2009, http://jitc.fhu.disa.mil/jitc_dri/pdfs/DoDaf_v2v1.pdf

DoD Discovery Metadata Specification (DDMS) v4.1, http://metadata.ces.mil

D0D Information Technology Standards Registry (DISR), https://DISRonline.csd.disa.mil

DoDD 4630.05, 23 April 2007, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

DoDD 5105.21, 18 March 2008, "Defense Intelligence Agency"

DoDD 5240.01 Series, 27 August 2007, "Defense Intelligence Activities"

DoDD 8320.02, 20 December 2004, "Data Sharing in a Net Centric Department of Defense"

DoDI 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

Intelligence Community Directive 501, 21 January 2009, "Discovery and Dissemination or Retrieval of Information Within the Intelligence Community"

Joint Publication 1-02, 12 April 2001 (as amended through 20 March 2006), "DoD Dictionary of Military and Associated Terms"

Joint Publication 2-0, 22 June 2007, "Joint Intelligence"

Joint Publication 2-01, 5 January 2012, "Joint and National Intelligence Support to Military Operations"

JROC Memorandum 039-10, 19 March 2010, "Joint Intelligence Operations Center Information Technology Enterprise Initial Capabilities Document"

Public Law 108-458, 17 December 2004, "Intelligence Reform and Terrorism Prevention Act of 2004"

USD(I) Memorandum, 6 December 2007, Staff Assistance Visit (SAV) Report on Joint Intelligence Operations Centers (JIOC)

USD(I) Memorandum, 28 March 2010, JIOC SAV Report Action Plan

USD(I) Memorandum, 18 April 2012, Defense Intelligence Information Enterprise

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

BA FCB	Battlespace Awareness Functional Capabilities Board
C2	Command and Control
C4	Command, Control, Communications, and Computer
CI	Counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNSSI	Committee on National Security Systems Instruction
COI	Communities of Interest
DCGS	Distributed Common Ground/Surface System
DDMS	DoD Discovery Metadata Specification
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoDAF	DoD Architecture Framework
DoDD	DoD Directive
DoDI	DoD Instruction
ER	ENTERPRISE RESOLVE
EXORD	Execute Order
GCCS-I3	Global Command and Control System - Integrated Imagery and Intelligence
IC	Intelligence Community
IC ITE	Intelligence Community Information Technology Enterprise
ISR	Intelligence, Surveillance, and Reconnaissance
IT	information technology
J-2	Joint Staff, Director of Intelligence
JEI	Joint Enterprise Integration
JICARS	Joint Intelligence Capabilities, Assessments, and Requirements System
JIE	Joint Information Environment
JIOC	Joint Intelligence Operations Center
JISF	Joint Information Sharing Forum
JRIC	Joint Reserve Intelligence Center
JROC	Joint Requirements Oversight Council

JS	Joint Staff
JWII	Joint Warfighter Intelligence Integration
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
ODNI	Office of the Director of National Intelligence
VCJCS	Vice Chairman of the Joint Chiefs of Staff

PART II—DEFINITIONS

Analysis and Production. In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (JP 2-01)

Battlespace Awareness. Knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather, and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply combat power, protect the force, and/or complete the mission. (JP 2-01)

Collection. The acquisition of information and the provision of this information to processing elements. (JP 2-01)

Collection Asset. A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02) In the context of this instruction, collection assets also include people involved in human intelligence activities.

Command and Control (C2) System. The facilities, equipment, communications, and personnel essential to a command for planning, directing, and controlling operations of assigned and attached forces pursuant to the missions assigned. (JP-60)

Communities of Interest (COI). A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and, therefore, must have shared vocabulary for the information it exchanges. (DODD 8320.02)

Consumer. Person or agency that uses information or intelligence produced by either its own staff or other agencies. (JP 2-01)

Counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

Cross-Domain Solution. An information assurance solution that provides the ability to access or transfer information between two or more security domains. (CNSSI No. 4009)

Discovery. Locating a resource on the enterprise, using a process (such as a search engine) to obtain knowledge of information content or services that exploit metadata descriptions of enterprise IT resources stored in directories, registries, and catalogs. (DDMS). The concept of discovery includes search, identification, retrieval, presentation, and accessibility functions and both "push" and "pull" capabilities.

Dissemination. The delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. (JP 2-01)

Department of Defense Information Enterprise. The DoD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life cycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems. (DoDD 8000.01)

DoD Intelligence Agencies. In the context of this instruction, the DoD Intelligence Agencies include the DIA, the NGA, the NSA/CSS, and the NRO.

ENTERPRISE RESOLVE (ER). In the context of this instruction, the Joint Staff, J-2-led ER campaign is a multi-venue, multi-year, and multi-partner integration effort intended to maximize numerous community testing venues, exercises, demonstrations, and other events to conduct operational assessments and to support enterprise testing focused on resolving intelligence sharing gaps and enterprise requirements identified through the JISF process.

Inaccessible Data. In the context of this instruction, inaccessible data is data that a consumer holds the privilege to access, but cannot due to: inconsistent policy, access control measures, firewalls, unsuitable levels of network service, or other similar impediment.

Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, systems view, and technical standards view) that facilitates data integration and promotes interoperability across family of systems and system of systems, and compatibility among related architectures. (CJCSI 3170.01F)

Intelligence. 1. The product resulting from the collection, processing, exploitation, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 2-01)

Intelligence Certification. The affirmation that requirements for intelligence support have been completely and adequately declared and identified; adequately assessed for projected supportability; that critical intelligence supportability or threat-related issues identified during coordination of program documents have been addressed; and that any projected shortcomings in intelligence support will be dealt with in an appropriate manner. (CJCSI 3312.01A)

Intelligence Community (IC). The IC includes the ODNI; the Central Intelligence Agency; the NSA; the DIA; the NGA; the NRO; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of the Treasury; the elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard; and such other elements of any other department or agency as may be designated by the President, or designated jointly by the DNI and the head of the department or agency concerned, as an element of the IC. (Public Law 108-458, Section 1073)

Intelligence Community IT Enterprise (IC ITE). In the context of this instruction, IC ITE moves the IC from an agency-centric IT architecture to a common platform where the Community easily and securely shares technology, information, and resources. The enterprise features a cloud-based architecture with a common platform and infrastructure (single IC desktop, an apps mall, and common back office design). IC ITE will operate primarily at the Protection Level 4 (PL 4) security enclave.

Interoperability. The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services such that this exchange enables them to operate effectively together. (DODD 4630.05)

Intelligence, Surveillance, and Reconnaissance (ISR). An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. (JP 2-01)

Joint Information Environment (JIE). A secure JIE, comprised of shared IT infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. (Charter for the JIE Management Construct, Nov 9, 2012.

Joint Information Sharing Forum (JISF). In the context of this instruction, the JISF provides a mechanism for DCGS, GCCS-I3 and JIOC operational users to introduce proposed enterprise-level requirements. External requirements introduced by IC governance bodies are processed by the JISF, as well. The JISF processes, consolidates, evaluates, vets, and prioritizes these requirements for resolution. The JISF monitors these enterprise-level requirements from introduction through resolution and provides user feedback.

Joint Intelligence Capabilities, Assessments, and Requirements System (JICARS). In the context of this instruction, the JICARS is a Joint Staff, J-2-led system that provides an overarching process to conduct rigorous and unbiased assessments of JROC approved requirements and proposed solutions for data integration, application/tool interoperability, and information sharing across the CCMDs, Services, and the National/DoD Intelligence Agencies (DIA, NGA, NSA/CSS, NRO). The JICARS, JISF and its supporting ER campaign series were established as the primary mechanism to synchronize efforts for information system requirements, capabilities, and assessments at the enterprise level.

Joint Intelligence Operations Center (JIOC). A functional capabilities construct established at each CCMD and USFK to plan, prepare, integrate, direct, synchronize, and manage full-spectrum Defense Intelligence operations. JIOCs seamlessly integrate all DoD intelligence functions and disciplines and ensure all sources of intelligence are made available across the DoD to positively affect U.S. military operations. (JIOC EXORD)

Joint Warfighter Intelligence Integration (JWII). In the context of this instruction, JWII is the set of processes and actions undertaken with the intent to synchronize, correlate, and deliver national security community data across IC architectures enabling seamless access, configuration, manipulation and employment of systems benefitting the execution of the national military strategy.

Metadata. Descriptive information about the meaning of other data, typically embedded in a document or product. Metadata can be provided in many forms, including Extensible Markup Language providing the means for effective database querying. (DoD Net-Centric Data Strategy)

Multi-Level Security. Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. (CNSSI 4009)

National Repository. In the context of this instruction, the National Repository is accessible data storage established by a DoD Intelligence Agency. The *national* characterization applies to governance assigned at the national level, and not to data type, location, or access.

National Security Community. In the context of this instruction, the organizations currently under the purview of the DNI, the Secretary of Defense, the Secretary of Homeland Security, and the Attorney General.

Net-Centric. Exploitation of advancing technology, such as interoperable forms of data access found in cloud computing, that moves from an applications-centric to a data-centric paradigm – that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components. (CJCSI 6212.01D)

Operational Constraint. In the context of this instruction, operational constraints are the budgetary, resource, or technological limitations or policy restrictions that influence ongoing operations. Operational constraints can be temporary in nature (e.g., insufficient equipment, manning, or power) or permanent in nature (e.g., equipment design, policy restrictions, and durability considerations).

Originator Controlled. A dissemination control marking used on classified intelligence that clearly identifies, or reasonably would permit ready identification of intelligence sources or methods that are particularly susceptible to an unacceptable level of risk. Information bearing this marking may be disseminated within the HQ and specified subordinate elements of the recipient organizations, including their contractors within government facilities. This information may also be incorporated in whole or in part into other briefings or products, provided the briefing or product is presented or distributed only to original recipients of the information. Dissemination beyond HQ and specified subordinate elements or to agencies other than the original recipients requires advanced permission from the originator. (DCID 6/6)

Processing and Exploitation. The conversion of collected information into forms suitable to the analysis and production of intelligence. (JP 2-01)

Sensor. In the context of this instruction, refers to an asset used for intelligence collection. See *Collection Asset*.

Service. A Service is a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistently within constraints and policies as specified by the service description. (DoD Net-Centric Services Strategy)

Shared Space. A Shared Space is a mechanism that provides storage of and access to data for users within a bounded network space. Enterprise-shared space refers to a store of data that is accessible by all users within or across security domains on the GIG. A shared space provides virtual or physical access to any number of data assets (e.g., catalogs, Web sites, registries, document storage, and databases). (DoD Net-Centric Data Strategy)

Socio-cultural Information. The social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (JP 1-02)

Standard. A formal agreement documenting generally accepted specifications or criteria for products, processes, procedures, policies, systems, and/or personnel. (American National Standards Institute)

Tagging. In the context of this instruction, tagging refers to an approach to identify and use metadata elements either embedded in or related to a data asset that will enable high precision and high recall search and retrieval.

Undiscoverable Data. In the context of this instruction, undiscoverable data is data that a consumer holds the privilege to access, but cannot because there is no way for the consumer to know that the data exist.

Warfighter Intelligence. In the context of this instruction, warfighter intelligence is intelligence and CI data collected using multiple domains and collection disciplines at the strategic, operational and tactical levels, and the products resulting from the exploitation, analysis and fusion of collected intelligence data.