

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

Directive current as of 1 Aug 2011

J2
DISTRIBUTION: A, B, C, J, S

CJCSI 3340.02A
16 November 2008

HORIZONTAL INTEGRATION OF WARFIGHTER INTELLIGENCE

References: See Enclosure C.

1. Purpose. The purpose of this instruction is to establish policy and procedures for improving the horizontal integration (HI) of warfighter intelligence data.

a. HI is the set of processes and capabilities to acquire, synchronize, correlate, and deliver national security community data with responsiveness to ensure success across all policy and operational missions.

b. Horizontally integrating warfighter intelligence data improves the consumers' production, analysis and dissemination capabilities. HI requires access (including discovery, search, retrieval, and display) to intelligence data among the warfighters and other producers and consumers via standardized services and architectures. These consumers include, but are not limited to, the combatant commands, Services, Defense agencies, and the Intelligence Community.

2. Cancellation. CJCSI 3340.02, 23 December 2005, "Horizontal Integration of Warfighter Intelligence," is cancelled.

3. Applicability. This instruction applies to:

a. The Services (including the Service intelligence centers), combatant commands, and the Joint Staff.

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. All counterintelligence (CI) activities/agencies within the DOD.

d. Warfighter intelligence data, defined as intelligence data collected by assets (overhead, airborne, terrestrial, sea-based, undersea and human) 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 Enclosure A to include Joint Intelligence Operation Center principles and Defense Intelligence policy and guidance (more accurate reflection of the current state of play for enterprise architectures crossing all domains). Deleted superfluous graphical depictions.

b. Added responsibilities of Director, Defense Intelligence Agency, and expanded roles and responsibilities of other entities.


c. Updated references to include most recent revisions and added current applicable guidance or directives.

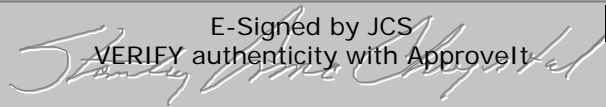
d. Added pertinent definitions to glossary.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), 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:

E-Signed by JCS
VERIFY authenticity with ApproveIt 



Enclosures:

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

(INTENTIONALLY BLANK)

DISTRIBUTION

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

	<u>Copies</u>
Under Secretary of Defense for Acquisition, Technology and Logistics	2
Under Secretary of Defense for Intelligence	2
Assistant Secretary of Defense (Network & Information Integration)/DOD CIO	2
Director, Program Analysis and Evaluation	2
Director, National Reconnaissance Office	2
Director of National Intelligence	2

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY

1. DOD policy, standing Execute Orders, and Joint Intelligence Operations Center (JIOC) principles specify that broad access to collected intelligence will be provided via an enterprise and horizontally integrated approach that ensures an uninhibited flow of information from all sources and databases.
2. Joint doctrine (reference b) specifies that joint forces have access to national intelligence capabilities to improve in-theater analysis and production processes, both now and in the future.
3. To improve the HI of warfighter and national intelligence data, intelligence activities must implement data sharing among intelligence capabilities, agencies, processes, and personnel using an enterprise-oriented, data interoperable approach in accordance with DOD/DNI directives, and consistent with applicable security policies. This strategy and HI focus must incorporate cross-domain architectures of the Distributed Common Ground System (DCGS)/DCGS Integrated Backbone, Regional Service Centers, the Defense Intelligence Operations Coordination Center (DIOCC), JIOCs, National Intelligence Agencies/Combat Support Agencies (CSA), and key partner nations (where applicable).
4. In the objective operating state, all sensor data is made accessible using repeatable, standardized processes and enterprise HI architectures, including tagging of the data for discovery. The standard for discovery tagging is the DOD Discovery Metadata Specification (DDMS, reference h). Organizations accessing intelligence data invoke the discovery processes to locate and access the data via standards-based services. Organizations conducting processing, exploitation, analysis, and production activities use repeatable processes and composable, standards-based services.
5. The Commands/JIOCs, Services, DOD intelligence agencies, and the DIOCC will develop capabilities to migrate the current intelligence data environment (and associated architectures) toward a future enterprise and HI approach for the conduct of intelligence operations.
 - a. The Commands/JIOCs, Services, DOD intelligence agencies, and the DIOCC will establish an HI and seamless data sharing enterprise/architecture in accordance with the Defense Intelligence Strategy, JIOC/DIOCC EXORD and other applicable directives.

b. The DOD intelligence agencies will establish national repositories to store warfighter intelligence data that would otherwise be undiscoverable and inaccessible to consumers outside the theater. 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.

c. Existing architectures will be updated to identify the data's earliest point of consumability (EPofC). Data will be tagged with metadata at the source, or at the closest operationally and technically feasible point, to enable its common visibility. Standards-based services will be provided at the EPofC for access prior to and during analysis. The EPofC shall be documented within the SV-4 Data Flow Diagram (reference i) by identifying the system function where data is discoverable, definable, and accessible.

d. The DOD intelligence agencies and Services will develop publishing mechanisms that are compliant with service-orientated architecture (SOA) cross-database search and retrieval standards to enable federated discovery and access. This capability promotes joint force interoperability with present and future mission partners (federal agencies, law enforcement, multinational, and others).

e. Rule Sets, as outlined in Joint Requirements Oversight Council Memorandum (JROCM) 124-04 (reference j), describe key sensor attributes, minimum capabilities, or available information required to enable integration and fusion of data from multiple sources. In accordance with CJCS Series 3170 (reference k), these performance attributes will be:

(1) Identified through the Joint Capabilities Integration and Development System (JCIDS) analysis process.

(2) Documented in initial capabilities documents (ICD).

(3) Expressed in capability development documents (CDD) and capability production documents (CPD) as key performance parameters (KPP) and additional attributes.

f. Future architectures will incorporate DCGS/DCGS Integration Backbone, Regional Service Centers, JIOCs, National Intelligence Agencies/CSA, the DIOCC, Joint Reserve Intelligence Centers capabilities and key partner nations (where applicable). They will maximize the use of multi-level security (MLS) capabilities to:

(1) Reduce overall cross-domain solution (CDS) footprint, proliferation of guards, and associated manpower and sustainment requirements.

- (2) Improve efficiency of automated tearline release.
 - (3) Support data aggregation needed for advanced analysis and fusion.
 - (4) Eliminate unnecessary data duplication.
 - (5) Improve adaptability of data sources to new dissemination requirements.
 - (6) Better enforce mandatory access control based on identity and privilege.
6. Adherence to well-defined information technology (IT) standards is critical to horizontally integrating warfighter intelligence data. Service, combatant command, and DOD intelligence agency participation in the DOD-chartered standards management body, the Information Technology Standards Committee (ITSC), is essential to a productive capabilities development environment and an interoperable intelligence enterprise. Thorough coordination of proposed data standards among ITSC participants in a community of interest (COI) approach (reference d) is necessary to reduce fiscal impacts during implementation.
7. The Services, combatant commands, and DOD intelligence agencies will continue to resolve conflicts in metadata standards through the change request process of the ITSC (reference l) and participation in the Intelligence Community Information Sharing - Metadata Standards Team (reference m).
8. The Services, combatant commands, and DOD intelligence agencies will work to achieve semantic agreement on their vocabularies through existing COIs, and future COIs, as required.
9. This policy does not alter combatant commanders' and Service Chiefs' existing C2 authorities and responsibilities concerning organic theater intelligence, surveillance, and reconnaissance collection assets. Access to shared data must not interfere with ongoing theater operations.

(INTENTIONALLY BLANK)

ENCLOSURE B
RESPONSIBILITIES

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

a. Evaluate compliance with this instruction and USD(I) policy through the Battlespace Awareness Functional Capabilities Board (BA FCB) assessment processes and Joint Military Intelligence Requirements Certification (reference n).

b. Represent the BA domain as a member of the ITSC.

c. Adjudicate conflicts in metadata agreements and identifying authoritative sources in accordance with reference c.

d. Provide functional expertise to IT standards working groups, technical working groups, and other COIs as required.

e. Validate EPofC documentation in integrated architectures as a part of intelligence certification (reference n).

f. Adjudicate operational constraints on access to warfighter intelligence data between DOD intelligence agencies and combatant commands.

g. Represent the intelligence information sharing equities of the combatant commands and Services at the Information Sharing Policy Coordinating Committee (IS PCC), in synchronization with the Joint Staff/J-5 lead and in coordination with the OUSD(I). Ensure the policies and implementation of information sharing initiatives and objectives as outlined in the DOD Information Sharing Strategy, associated Implementation Plan and the Defense Intelligence Strategy support HI of warfighter intelligence with present and future mission partners.

h. In conjunction with DIA, the DIOCC and USJFCOM, develop a methodology to assess the efficacy of Defense Intelligence HI support to operational objectives and recommend changes to address shortfalls to the CJCS and the OUSD(I).

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

a. Provide comprehensive IT infrastructure support to the combatant commands/JIOCs through Regional Service Centers (RSC) and serve as the primary enabler for HI and inter-combatant command IT coordination.

b. Develop and implement a systems architecture and HI plan for the DIOCC, combatant commands/JIOCs, and associated Joint Reserve Intelligence Centers consistent with DOD and the ODNI information sharing environment initiatives. Architecture should include cross-domain capabilities, the DCGS/DCGS Integration Backbone, RSCs, National Agencies/CSAs, and key partner nations (where applicable).

c. Facilitate access to CSA databases for the combatant commands/JIOCs, and serve as the DOD conduit for interagency IT connectivity and interoperability. Where possible, also facilitate information and/or data access for allies and coalition partners.

d. Annually assess success of information sharing and HI initiatives between the combatant commands/JIOCs, CSAs, National Intelligence Agencies, Reserve Components, and appropriate Allies and Coalition Partners and provide recommendations to maximize HI via the CJCS and USD(I) to the Secretary of Defense or designated representatives and DNI for action.

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

f. Adjudicate operational constraints on access to warfighter intelligence data between DOD intelligence agencies and the combatant commands/JIOCs via the DIOCC and National Intelligence Coordination Center (NIC-C).

3. Directors of the DOD intelligence agencies will:

a. Ensure emerging capabilities enable enterprise and standards-based services for access to data, adhere to COI-developed semantic agreements, and adhere to standards-based, approved interfaces with other shared spaces such as those available via DCGS, Intelink, or stored in a RSC, National Data Center (NDC), or Cryptologic Center (CC).

b. Establish and manage national repositories to access warfighter intelligence data that is otherwise undiscoverable and inaccessible to consumers outside the theater.

c. Assist combatant commands in developing procedures for tagging data with discovery metadata and making data accessible via standards-based services from national repositories (reference paragraph 4.c.).

d. Ensure all DOD intelligence agency capabilities that produce intelligence data:

(1) Tag their information with discovery metadata at the source, or the closest operationally and technically feasible point.

(2) Provide standards-based services for access to data at the EPofC.

(3) Document the EPofC in the integrated architectures of capability documents submitted through JCIDS after the effective date of this publication.

e. Ensure rule sets and standards are included in all appropriate JCIDS documents to maximize data sharing and usability.

f. Provide functional expertise to IT standards working groups, technical working groups, and COIs as required.

g. Develop and advocate enterprise and standards-based approaches to system and data interoperability with present and future mission partners in support of the combatant commands/JIOCs and Services. Use COI approaches to gain semantic agreement on vocabularies, as necessary.

h. Develop and maintain education and training required to implement HI policy and procedures.

4. Chiefs of the Military Services will:

a. Ensure emerging capabilities provide enterprise and standards-based services for access to data, adhere to COI-developed semantic agreements, adhere to standards-based, approved interfaces with other shared spaces such as those available via DCGS, Intelink, or stored in a RSC, NDC, or CC.

b. Ensure all Service capabilities that produce intelligence data:

(1) Tag their information with discovery metadata at either the source or the closest operationally and technically feasible point.

(2) Provide standards-based services for access to data at the EPofC.

(3) Document the EPofC in the integrated architectures of capability documents submitted through JCIDS after the effective date of this publication.

(4) Provide functional expertise to IT standards working groups, technical working groups, and COIs as required.

(5) Develop and maintain education and training required to implement HI policy and procedures.

c. Evaluate and recommend best HI processes and/or procedures for incorporation into the Defense Intelligence enterprise to the Joint Staff and OUSD(I).

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 components of national repositories as required by enterprise and/or DOD intelligence agencies' architectures.

c. Develop procedures for tagging data with discovery metadata and posting data to national repositories. For each type of data, coordinate with the authoritative DOD intelligence agency to produce business rules for:

(1) Identifying inaccessible and undiscoverable data.

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

(3) Determining the authoritative source(s).

(4) Mitigating operational constraints (e.g., bandwidth, guard capacity) and dissemination control measures (e.g. originator controlled (ORCON) above the tearline).

d. Develop and maintain education and training required to implement HI policy and procedures.

6. Commander, Joint Forces Command, will:

a. Conduct joint intelligence concept development and experimentation to identify future capabilities that enhance and enable data repositories and the horizontal integration of warfighter intelligence data.

b. Based on results from HI experimentation, recommend near-, mid-, and far-term cross-domain solutions (CDS) that enhance and enable the horizontal integration of warfighter intelligence data.

ENCLOSURE C

REFERENCES

- a. USD(I) memorandum, 10 February 2004, "Horizontal Integration of Collected Theater Intelligence"
- b. Joint Publication 2-01, 22 June 2007, "Joint and National Intelligence Support to Military Operations"
- c. Defense Intelligence Strategy, OUSD(I) Pamphlet, 2008
- d. DODD 8320.02, 2 December 2004, "Data Sharing in a Net-Centric Department of Defense"
- e. DOD Chief Information Officer, 9 May 2003, "DOD Net-Centric Data Strategy"
- f. DOD Chief Information Officer, 4 May 2007, "DOD Net-Centric Services Strategy"
- g. DOD Chief Information Officer, 4 May 2007, "DOD Information Sharing Strategy"
- h. DOD Deputy Chief Information Officer, 17 July 2008, "DOD Discovery Metadata Specification (DDMS) v2.0"
- i. DOD Architecture Framework Working Group, 23 April 2007, "DOD Architecture Framework v1.5"
- j. JROC memorandum 124-04, 9 July 2004, "Common Data Standards and Format to Enable Horizontal Integration (HI)"
- k. CJCSI 3170.01 Series, 1 May 2007, "Joint Capabilities Integration and Development System"
- l. DOD IT Standards Committee (ITSC) Standard Operating Procedures, 26 October 2004
- m. Intelligence Community Information Sharing - Metadata Standards Team, <https://www.dnidata.org>
- n. CJCSI 3312.01 Series, 23 February 2007, "Joint Military Intelligence Requirements Certification"
- o. Public Law 108-458, 17 December 2004, "Intelligence Reform and Terrorism

Prevention Act of 2004”

- p. DOD Metadata Registry v7.0, <https://metadata.dod.mil>
- q. Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, 12 April 2001 (as amended through 20 March 2006)
- r. CJCSI 6211.02C, 9 July 2008, “Defense Information System Network (DISN): Policy and Responsibilities”
- s. DODD 4630.05, 23 April 2007, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”
- t. CNSSI 4009, June 2006, “National Information Assurance (IA) Glossary”
- u. DODI 4630.8, 30 June 2004, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”
- v. DCID 6/6, 30 June 1998, “Security Controls on the Dissemination of Intelligence Information”
- w. CJCSI 6212.01 Series, 8 March 2006, “Interoperability and Supportability of Information Technology and National Security Systems.”
- x. Executive Order 13388 of October 25, 2005, “Further Strengthening the Sharing of Terrorism Information To Protect Americans”
- y. Director of National Intelligence memorandum E/S 00245, 22 July 2005, “Direction for Measurement and Signature Intelligence Management”
- z. Director of Central Intelligence Directive 8/1, 4 June 2004, “Intelligence Community Policy on Intelligence Information Sharing”
- aa. Intelligence Community Chief Information Officer Executive Council, 15 April 2003, “Intelligence Community Policy for Metadata and Metadata Markup”
- bb. CJCS Execute Order (EXORD), Joint Intelligence Operations Center (JIOC), 031640Z April 2006
- cc. CJCS EXORD, Defense Intelligence Operations Coordination Center (DIOCC), 042130Z December 2007, as amended by VCJCS EXORD mod 1, 151730Z February 2008

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

ee. USD(I) Memorandum, 28 March 2008, JIOC SAV Report Action Plan

(INTENTIONALLY BLANK)

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

BA	Battlespace Awareness
CDD	Capability Development Document
CDS	Cross-Domain Solution
CES	Core Enterprise Services
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	Community of Interest
CPD	Capability Production Document
DCGS	Distributed Common Ground System
DDMS	DOD Discovery Metadata Specification
DIA	Defense Intelligence Agency
DIOCC	Defense Intelligence Operations Coordination Center
DGS	Distributed Ground System
DNI	Director of National Intelligence
DODAF	DOD Architecture Framework
DODD	DOD Directive
DODI	DOD Instruction
DODIIS	DOD Intelligence Information System
EPofC	Earliest Point of Consumability
FCB	Functional Capabilities Board
GIG	Global Information Grid
HI	Horizontal Integration
IC	Intelligence Community
ICD	Initial Capabilities Document
IS PCC	Information Sharing Policy Coordinating Committee
ISE	Information Sharing Environment
IT	Information Technology
ITSC	IT Standards Committee
JCIDS	Joint Capabilities Integration and Development System
JIOC	Joint Intelligence Operations Center
JP	Joint Publication

JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
KPP	Key Performance Parameter
MLS	Multi-Level Security
NCES	Net-Centric Enterprise Services
NDC	National Data Center
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
ORCON	Originator Controlled
RSC	Regional Service Center
SIGINT	Signals Intelligence
SOA	Service Oriented Architecture
SV	Systems View
USD(I)	Undersecretary of Defense for Intelligence
XML	Extensible Markup Language

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 include people involved in human intelligence activities.

Community 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 (CDS). An information assurance solution that provides the ability to manually and/or automatically access and/or transfer between two or more differing security domains. (CJCSI 6211.02C)

Defense Intelligence Operations Coordination Center (DIOCC). A Defense-level intelligence operations coordination center established to plan, integrate, coordinate, direct, synchronize, and manage full-spectrum Defense Intelligence operations and capabilities, to include Defense collection management and ISR, in support of the combatant commands/JIOCs to satisfy the priorities of the DOD and the Nation. The DIOCC maintains a support relationship, as an interagency partner, with the DNI National Intelligence Coordination Center (NIC-C) to coordinate Defense and National Intelligence capabilities/activities. (DIOCC EXORD)

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 information technology resources stored in directories, registries, and catalogs. (DOD Discovery Metadata Specification). 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)

DOD Intelligence Agencies. 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).

Earliest Point of Consumability (EPofC). In the context of this CJCSI, the point at which data is tagged with discovery metadata. No system functions prior to this point in the data flow require discovery services to locate the data. At least one system function after this point has data tagged for discovery as a necessary condition for execution. Data may be acted upon by processes prior to the EPofC (including other types of tagging), but enterprise knowledge of its existence is not possible.

Horizontal Integration (HI). Processes and capabilities to acquire, synchronize, correlate, and deliver National Security Community data with responsiveness to ensure success across all policy and operational missions.

Inaccessible Data. In the context of this CJCSI, 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 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, 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 Office of the Director of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; 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 Director of National Intelligence and the head of the department or agency concerned, as an element of the Intelligence Community. (Public Law 108-458, Section 1073)

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 so exchanged to enable 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. This is an integrated intelligence and operations function. (JP 2-01)

Joint Intelligence Operations Center (JIOC). An intelligence operations center established at each combatant command 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 effect U.S. military operations. (JIOC EXORD)

Transformational Joint Intelligence Operations Center (JIOC-X). Established at USJFCOM, JIOC-X conducts JIOC concept development, experimentation, and Joint Training, defining and incorporating best practices/processes and assessments in support of the DIOCC and combatant command JIOCs. JIOC-X also integrates JIOC operations and capabilities into Joint and/or combined exercises. (JIOC EXORD)

Metadata. Descriptive information about the meaning of other data. Metadata can be provided in many forms, including Extensible Markup Language (XML). (DOD Net-Centric Data Strategy)

Multi-Level Security (MLS). 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, 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 horizontal integration, the organizations currently under the purview of the Director of National Intelligence, the Secretary of Defense, the Secretary of Homeland Security, and the Attorney General.

Net-Centric. Exploitation of advancing technology 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)

Net-Centric Enterprise Services. An acquisition program that identifies, develops, and implements Global Information Grid Core Enterprise Services (GIG CES). GIG CES includes application, discovery, user assistant, collaboration, storage, mediation, messaging, enterprise service management, and information assurance/security. (DODI 4630.8)

Operational Constraint. In the context of this instruction, the 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, durability considerations).

Originator Controlled (ORCON). 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 countermeasures that would nullify or measurably reduce their effectiveness. 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 production of intelligence. (JP 2-01)

Schema. A diagrammatic representation, an outline, or a model. In relation to data management, a schema can represent any generic model or structure that deals with the organization, format, structure, or relationship of data. (DOD Net-Centric Data Strategy)

Sensor. In the context of this instruction, sensor refers to an asset used for

intelligence collection. See *Collection Asset*.

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

Service Oriented Architecture. A paradigm for defining, organizing, and utilizing distributed capabilities in the form of loosely coupled software services that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects that are consistent with measurable preconditions and expectations. (DOD Net-Centric Services Strategy)

Shared Space. 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)

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

Systems View 4 (SV-4). The systems functionality description documents system functional hierarchies and system functions, and the system data flows between them. The primary purposes of SV-4 are to: (1) develop a clear description of the necessary system data flows that are input (consumed) by and output (produced) by each system; (2) ensure that the functional connectivity is complete (i.e., that a system's required inputs are all satisfied); and (3) ensure that the functional decomposition reaches an appropriate level of detail. (DODAF v1.5, Volume II)

Tagging. In the context of this CJCSI, 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 CJCSI, data that a consumer holds the privilege to access, but cannot because there is no way for the consumer to discover that the data exists.

Warfighter Intelligence Data. Intelligence data (including CI) collected by assets (overhead, airborne, terrestrial, sea-based, undersea, and human) at the strategic, operational and tactical levels; and the products resulting from analysis and fusion of collected intelligence data.

(INTENTIONALLY BLANK)