Department of Defense

# INSTRUCTION

NUMBER 8110.1

February 6, 2004

ASD(NII)/DoD CIO

SUBJECT: Multinational Information Sharing Networks Implementation

References: (a) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(b) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(c) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)), February 12, 1992
(d) Sections 1425, 2223 and 5142 of the Clinger-Cohen Act of 1996 (Public Law 104-106) (40 U.S.C. Section 1401), February 10, 1996
(e) through (g), see enclosure 1

## 1. PURPOSE

This Instruction:

1.1. Implements policy under reference (a); establishes the Multinational[1] Information Sharing (MNIS) Program within the Department of Defense; and designates the MNIS Combined Enterprise Regional Information Exchange System (MNIS CENTRIXS) as the DoD standard for multinational information sharing networks using the Global Information Grid (GIG).

[1] For the purposes of this Instruction "multinational" includes all interactions with foreign nations whether they be referred to as combined, coalition, allied, bilateral, multilateral, or similar terminology.

1.2. Assigns responsibilities and provides procedures to standardize the means for connecting the DoD Components electronically to foreign nations on an Enterprise basis, and for allowing the secure, mutual exchange of operational and intelligence information in support of combined planning, a unity of effort, and decision superiority in multinational military operations.

1.3. Provides the guidance, framework, key principles, and interoperability processes for multinational information sharing networks, computing, information assurance, information management, and network management, to include their interoperability, that are part of the GIG.

## 2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to:

2.1.1. The Office of the Secretary of Defense, the Military Services, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components"). The term "Military Services," as used above, refers to the Army, the Navy, the Air Force, and the Marine Corps.

2.1.2. All DoD-owned or -controlled information systems (of the Combatant Commands, the Joint Chiefs of Staff (JCS), or any DoD Component) using Internet Protocol networks that exchange classified DoD information with foreign nations up to the SECRET classification level for the purpose of support to multinational military operations. Exceptions may be granted by the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) in accordance with this Instruction.

2.2. Nothing in this Instruction shall alter or supercede the existing authorities and policies of the Director of Central Intelligence, the Director of the National Security Agency (NSA), or the Director of the Defense Intelligence Agency regarding the exchange of Sensitive Compartmented Information and special access programs for intelligence as directed by Executive Order 12333 (reference (b)) and other related laws and regulations. In addition, this Instruction does not apply to the international information exchange systems of the NSA for any level of classified information.

2.3. This Instruction does not apply to the integral parts of weapons systems (e.g., datalinks such as Link 16) as defined by DoD Directive 5137.1 (reference (c)) or other

Information Technology (IT) components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a weapons systems mission performance or to its interfaces to other legacy systems.

## 3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

## 4. POLICY

This Instruction implements policy established in reference (a) for multinational information sharing networks using the GIG.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) shall:

5.1.1. Monitor, evaluate and provide advice to the Office of the Secretary of Defense in conjunction with the Chairman of the Joint Chiefs of Staff, regarding DoD MNIS network matters in accordance with sections 1425 and 2223 of the Clinger-Cohen Act of 1996 (reference (d)).

5.1.2. Act as the DoD lead and focal point for the MNIS Program as executed by the MNIS Program Management Office (MNISPMO).

5.1.3. Ensure that the MNISPMO manages the DoD MNIS network program and standard (known as MNIS CENTRIXS) based on the immediate operational needs of the DoD Components.

5.1.4. Oversee appropriations earmarked for the MNIS Program within the scope of this Instruction.

5.1.5. Develop and promulgate additional guidance consistent with this Instruction regarding MNIS CENTRIXS networks to address such topics as:

5.1.5.1. Network standards, procedures, and management;

5.1.5.2. The development and use of multi-level security (MLS), Communities Of Interest (COI), virtual private networks (VPN), and privacy mechanisms on these networks in conjunction with the NSA and other organizations; and,

5.1.5.3. Support to the automation of various foreign disclosure mechanisms and procedures to reduce the latency of interfaces and increase the effectiveness of information exchange with foreign nations over these networks.

5.1.6. Promulgate the MNIS CENTRIXS network standard that is certified in accordance with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) by DoD Instruction 5200.40, reference (e) or its revisions and supporting manuals.

5.1.7. Ensure the integration of MNIS CENTRIXS networks into the operation of existing DoD general service networks as a service to the Combatant Commands and other authorized network users.

5.1.8. Coordinate with the Chairman of the Joint Chiefs of Staff and the Commander, U.S. Joint Forces Command regarding the validated requirements of the Combatant Commands.

5.1.9. Designate an appropriate official to serve as the Designated Accreditation Authority (DAA) for the global MNIS CENTRIXS network and its standard as appropriate in accordance with the DITSCAP or its revisions.

5.1.10. Appoint the MNIS Program Manager in coordination with the Chairman of the Joint Chiefs of Staff.

5.1.11. Adjudicate exceptions submitted by the Joint Staff, Combatant Commands, Defense Agencies, or other DoD Components to the use of the MNIS CENTRIXS network standard for the exchange of DoD information with foreign partners after the exception has been coordinated with the MNISPMO.

5.1.12. Ensure the Director, Defense Information Systems Agency (DISA):

5.1.12.1. Integrates MNIS CENTRIXS networks into existing DoD general service communications infrastructure as a separate network (e.g., cmil.mil) servicing all DoD multinational information-sharing requirements within the scope of this Instruction.

5.1.12.2. Supports the MNISPMO in maintaining visibility on global MNIS CENTRIXS network operations to include security provisions at the appropriate level of detail from a central point (CENTRIXS Network Control Center (CNCC)), through a global MNIS CENTRIXS network management picture.

5.1.12.3. Integrates MNIS CENTRIXS networks into its information assurance (IA) processes for layered protection of networks and information to include development, identification, type-accreditation and implementation of all Computer Network Defense initiatives.

5.1.12.4. Conducts interoperability testing on all components of MNIS CENTRIXS networks to insure compliance with interoperability requirements.

5.1.12.5. Participates in the configuration management processes being implemented by the MNISPMO.

5.1.12.6. Provide Enterprise network intrusion detection, information assurance vulnerability alerts (IAVA), and DoD Computer Emergency Response Team (CERT) functions in support of MNIS CENTRIXS networks. In close coordination with Joint Task Force-Computer Network Operations (JTF-CNO), DoD Computer Emergency Response Team (DoD-CERT), and MNISPMO, develop a method by which vulnerability compliance status of all MNIS CENTRIXS networks shall be established and disseminated to the DoD community.

5.1.13. In coordination with the Chairman of the Joint Chiefs of Staff and the Commander, U.S. Joint Forces Command, designate an MNIS Executive Agent by April 1, 2004.

5.2. The Under Secretary of Defense for Intelligence provides direction and guidance to DoD Components regarding the operational use of intelligence to include its storage, processing, transmission, and dissemination on DoD secure networks, to include MNIS CENTRIXS networks.

5.3. The Heads of the DoD Components shall:

5.3.1. Support multinational information sharing network projects and programs within the scope of this Instruction. Provide the MNISPMO and ASD(NII)/DoD CIO project and planning information, as appropriate, to insure adherence to MNIS CENTRIXS network standards.

5.3.2. Use the MNIS CENTRIXS network standard as defined by this Instruction and the MNISPMO for all classified networks up to the SECRET level of classification for the exchange of information with foreign nations unless an exception is authorized by the ASD(NII)/DoD CIO.

5.3.3. Plan, program, budget, and execute funding to support the MNIS Program and MNIS CENTRIXS networks used by their organization, forces, or the Combatant Commands. Provide program and budget data regarding MNIS CENTRIXS to the MNISPMO.

5.4. The Chairman of the Joint Chiefs of Staff shall:

5.4.1. Develop, coordinate, and promulgate policies, doctrine, and procedures for the use of MNIS CENTRIXS networks for joint and combined operations.

5.4.2. Facilitate the evolutionary development of future evolutions of the MNIS CENTRIXS network standard.

5.4.3. Facilitate, through the Chairman of the Joint Requirements Oversight Council and the Commander, U.S. Joint Forces Command, the continued validation and integration of evolving multinational information exchange requirements/capabilities in MNIS CENTRIXS networks.

5.4.4. Coordinate with the ASD(NII)/DoD CIO on the appointment of a MNIS Program Manager.

5.4.5. Participate in multinational forums like Combined Communications Electronics Board (CCEB) and Multinational Interoperability Council (MIC) and coordinate appropriate actions (those within the purview of this Instruction) with MNISPMO and the U.S. Joint Forces Command (JFCOM).

5.4.6. Collect and validate multinational requirements for information systems used to exchange classified DoD information with foreign nations and provide these as inputs to the ASD(NII)/DoD CIO and the MNISPMO to assist in the development, acquisition, deployment, operations, and sustainment of MNIS CENTRIXS networks.

5.4.7. Coordinate with the ASD(NII) and the Commander, U.S. Joint Forces Command on the identification and designation of an MNIS Executive Agent by April 1, 2004.

5.5. The Commander of Combatant Commands shall:

5.5.1. Use the MNIS CENTRIXS network standard as defined by the MNISPMO and this Instruction for networks that exchange classified DoD information with foreign nations up to the SECRET classification level unless an exception is coordinated through the MNISPMO and authorized by the ASD(NII)/DoD CIO.

5.5.2. Maintain regional operational oversight and integrate the operation and management of MNIS CENTRIXS networks into support of regional combined operations.

5.5.3. Implement the MNIS CENTRIXS type-accredited information systems on MNIS CENTRIXS networks. Combatant Commands shall ensure subordinate commands utilize the MNIS CENTRIXS network standard type-accreditation. When the Combatant Command or subordinate command must deviate from the approved baseline, the Combatant Command shall submit a request to the MNISPMO for appropriate interoperability testing, certification, and accreditation of the information system. Combatant Commands and their components are responsible for accreditation of their implementations of MNIS CENTRIXS networks.

5.5.4. Use the NDP-1 (reference (f)) when exchanging classified information with foreign nations as well as appropriate information release procedures for unclassified information using MNIS CENTRIXS networks.

5.5.5. Provide a regional MNIS CENTRIXS network management feed to the DISA and the CPMO, as required for selected MNIS CENTRIXS networks, in the prescribed format, for use in global MNIS CENTRIXS network visibility.

5.5.6. Participate in the immediate operational needs and configuration management processes implemented by the MNISPMO for MNIS CENTRIXS networks.

5.5.7. Implement the MNISPMO Information Management process to develop and ensure a coordinated information management structure and procedures to ensure information accessibility on the global MNIS CENTRIXS networks.

5.5.8. Establish and maintain a MNIS CENTRIXS Enterprise infrastructure separate from the headquarters and remote site local area networks. This multinational enterprise environment shall serve as the regional services hub (where appropriate) in a hierarchical architecture, with the DoD global environment bridging Combatant Commands. Also, establish and operate a network operations center for the management and coordination of selected MNIS CENTRIXS networks within their Area of Responsibility (AOR).

5.6. The Commander, U.S. Joint Forces Command, shall:

5.6.1. In accordance with direction from the Chairman of the Joint Chiefs of Staff develop policies, doctrine, and procedures for the use of MNIS CENTRIXS networks for joint and combined operations, and facilitate the evolutionary development of the MNIS CENTRIXS standard. Integrate MNIS CENTRIXS into the Standing Joint Force Headquarters and Deployable Joint Command and Control Systems.

5.6.2. Collect and validate Combatant Command requirements for information systems used to exchange DoD information with foreign nations in accordance with Management Initiative Decision (MID) 912 (reference (g)) as it regards Joint Battle Management Command and Control (JBMC2); provide these as inputs to the ASD(NII)/DoD CIO and the MNISPMO to assist in the development, acquisition, deployment, operations, and sustainment of MNIS CENTRIXS networks.

5.6.3. Coordinate with the ASD(NII)/DoD CIO and the MNISPMO to ensure that the MNIS CENTRIXS network standard integrates C2 (Command and Control) planning and warfighting applications to support the Joint/Coalition Force Commander's equirements.

5.6.4. Provide coordinated input to the ASD(NII)/DoD CIO's management of the MNIS Program based on its roles and responsibilities for JBMC2.

5.6.5. Use MNIS CENTRIXS networks during joint exercises and experimentation to aid in the development of supporting doctrine, concepts of operation, and TTPs (Tactics, Techniques, and Procedures).

5.6.6. In consultation with the Combatant Commands, coordinate with the ASD(NII) and the Chairman of the Joint Chiefs of Staff on the identification and designation of an MNIS Executive Agent by April 1, 2004.

5.7. The Director, National Security Agency (NSA) shall:

5.7.1. Develop efficient, effective, and accreditable solutions for the connection of MNIS CENTRIXS networks to U.S. networks, and between/within various MNIS CENTRIXS network security and information domains.

5.7.2. Develop efficient, effective, and accreditable solutions for secure and dynamic COI and VPN capabilities, and information privacy services on MNIS CENTRIXS networks.

5.7.3. Assist in the development of accreditation documentation for the solutions recommended by the NSA for MNIS CENTRIXS networks and support certification testing in accordance with reference (e) or its revisions and supporting manuals.

5.8. The Multinational Information Sharing (MNIS) Program Manager shall:

5.8.1. Manage the MNIS Program and establish its programming and budgetary requirements to include facilitating the availability of adequate resources to migrate existing multinational information sharing network projects and programs to MNIS CENTRIXS network standards.

5.8.2. Establish and manage the MNIS CENTRIXS network standard based on the immediate operational needs of the Combatant Commands and the DoD Components, or/and validated operational requirements provided by the Commander, U.S. Joint Forces Command. The MNIS CENTRIXS network standard shall:

5.8.2.1. Permit any organization using the MNIS CENTRIXS standard to be globally interoperable with any other similar installation.

5.8.2.2. Maintain the appropriate levels of confidentiality, integrity, availability, authentication, and non-repudiation through the use of information assurance safeguards and operational procedures documented in the MNIS CENTRIXS network standard.

5.8.2.3. Be based on a common, or enterprise-level, communications and computing architecture to provide the mandated range of information and information management services.

5.8.2.4. Provide secure and dynamic COIs for allowing users to discretely separate categories of information and enforce need-to-know on the same virtual network.

5.8.2.5. Support deployable components for mobile combined operations with a rapid, flexible, reliable, and survivable "plug and play" capability.

5.8.2.6. Support regional network-centric nodes (Points of Presence) to support forward Combatant Command headquarters and split base operations.

5.8.2.7. Be integrated into the Standing Joint Force Headquarters and Deployable Joint Command and Control Systems.

5.8.3. Maintain a global MNIS CENTRIXS Network Control Center to monitor and support CENTRIXS network operations to include security provisions at the appropriate level of detail.

5.8.4. Establish and manage a network connection-approval process for MNIS CENTRIXS networks.

5.8.5. Provide for the type-security test and certification of MNIS CENTRIXS networks, their interfaces to each other, and their interfaces to U.S. networks, as appropriate, in accordance with reference (e), or its revisions, including primary responsibility for defining, validating, and promulgated security test and evaluation standards. The MNISPMO retains primary responsibility for acknowledging, managing, coordinating, and disseminating IAVA alerts, establishing corrective action plan, and reporting overall compliance to the JTF-CNO as a participant in the Vulnerability Management System (VMS).

5.8.6. Provide for the interoperability test and certification of MNIS CENTRIXS networks and their interfaces to each other, and to U.S. networks, in coordination with the Director, DISA.

5.8.7. Evolve the MNIS CENTRIXS network standard based on the immediate operational needs of the Combatant Commands and other DoD Components in conjunction with validated operational requirements provided by the U. S. Joint Forces Command.

5.8.8. Designate the Chairperson and manage the configuration management and engineering review boards for the MNIS CENTRIXS network standard to maintain the appropriate level of DoD standardization.

5.8.9. Coordinate exceptions to the use of the MNIS CENTRIXS network standard submitted by the Office of the Joint Chiefs of Staff, the Combatant Commands, the Defense Agencies, or other DoD Components for the exchange of DoD information with foreign partners.

5.8.10. Develop, coordinate, and promulgate procedures for the development, management, and the use of MNIS CENTRIXS networks.

## 6. PROCEDURES

6.1. The MNIS CENTRIXS network standard shall be managed by the MNISPMO. The multinational information sharing portion of the GIG, MNIS CENTRIXS, shall be "GIG compliant" in its configuration management, architecture, and operational implementation. MNIS CENTRIXS-equipped forces shall be able to "plug and play" anywhere in the World.

6.2. The MNIS CENTRIXS Network Standard:

6.2.1. All DoD multinational information sharing networks within the scope of this Instruction shall use and implement the common MNIS CENTRIXS network standard (networks, software, hardware, and interfaces). This shall enable U.S. Forces to flexibly, reliably, and securely exchange information with foreign nations on a worldwide basis, and reduce the number of duplicate, non-interoperable networks with similar functions.

6.2.2. The MNISPMO shall provide a standard type-tested, -certified, and -accredited configuration for the secure exchange of information with foreign nations. The MNISPMO is specifically responsible for, but not limited to, the type-accreditation of all guards and trusted-interface devices for implementation in MNIS CENTRIXS networks.

6.2.3. The MNIS CENTRIXS network standard shall be integrated into the operation of existing DoD general service networks and shall leverage Combatant Command existing multinational information sharing system/network capabilities where possible to support the Combatant Commands and other authorized users, and to develop the MNIS CENTRIXS standard.

6.2.4. The Combatant Commands shall operate their MNIS CENTRIXS enterprise networks regionally as an integrated element of the global MNIS CENTRIXS network.

6.3. Programming and Management: The MNISPMO shall manage the program supporting MNIS CENTRIXS. The ASD(NII), in coordination with the Chairman of the Joint Chief of Staff, shall issue implementation instructions on how to program funding for MNIS CENTRIXS networks.

6.4. Immediate Operational Needs/Operational Requirements Submission for MNIS CENTRIXS networks:

6.4.1. Immediate operational needs, requiring funding or decision support from the MNISPMO, for MNIS CENTRIXS networks shall be consolidated and validated by the Combatant Commands and submitted by record message or letter to the MNISPMO. The MNISPMO shall address these requirements within the confines of DoD policy and resources.

6.4.2. Operational requirements for future iterations of the MNIS CENTRIXS network standard shall be submitted as part of the established joint requirements processes through Commander, U.S. Joint Forces Command.

6.5. Cross-Command and Staff Coordination for the MNIS Program:

6.5.1. Coordination on MNIS and MNIS CENTRIXS matters must include the MNISPMO as an information addressee (as a minimum).

6.5.2. The MNISPMO shall chair a periodic MNIS CENTRIXS Cross-Command Conference.

6.6. Configuration Management (CM) of MNIS CENTRIXS Networks:

6.6.1. The MNISPMO shall establish a MNIS CENTRIXS CM process that shall address engineering review and CM. The CM Board shall include, as a minimum, the Combatant Commands and DISA. The Combatant Commands shall also conduct their own CM processes (within the overall CM process) within their areas of responsibility in accordance with the established MNIS CENTRIXS CM process.

6.6.2. The MNIS CENTRIXS CM process shall document the standards and their implementations; the MNISPMO shall publish them for use by all the DoD Components.

6.7. Management of Global Cryptographic Keying Material (KEYMAT): The MNISPMO shall establish procedures with the appropriate DoD Components to provide for the centralized management of global KEYMAT for MNIS CENTRIXS networks.

6.8. Management of Cryptographic Equipment: The MNISPMO shall be an information addressee on any messages from the DoD Components relating to the RIP (Release in Principle) and RIS (Release in Specifics), and allocation of U.S. cryptographic equipment for use in MNIS CENTRIXS networks.

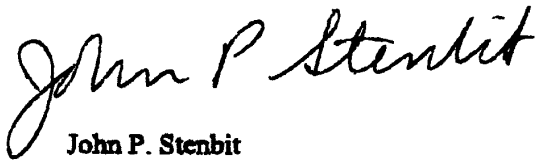
6.9. Classification of Material: The ASD(NII)/DoD CIO shall issue a classification guide regarding the classification of information about MNIS CENTRIXS (software,

hardware, architectures, configurations, etc.) networks. The release and proper classification of information published on or transmitted via MNIS CENTRIXS networks is the responsibility of the organization publishing or transmitting the information. Appropriate foreign disclosure procedures shall be used for classified material; and proper procedures for the release of unclassified material shall be observed.

6.10. Exceptions to the Use of the MNIS CENTRIXS Standard for DoD Information Exchange with Foreign Partners: The ASD(NII)/DoD CIO shall be the adjudication authority for an exception submitted by the Joint Staff, the Combatant Commands, the Defense Agencies, or other DoD Components for using the MNIS CENTRIXS network standard for the exchange of DoD information with foreign partners. Exceptions shall be submitted through the chain of command to the ASD(NII)/DoD CIO after coordination through the MNISPMO. Exceptions shall be granted when the services desired may not be provided via MNIS CENTRIXS networks for political, practical, resource, or technical reasons. All exceptions shall be submitted within 6 months of the effective date of this Instruction.

## 7. EFFECTIVE DATE

This Instruction is effective immediately.



**John P. Stenbit**
**Assistant Secretary of Defense for Networks,**
**And Information Integration/Department of Defense**
**Chief Information Officer**

Enclosures - 2

E1. References, continued

E2. Definitions

## E1. ENCLOSURE 1

## REFERENCES, continued

(e) DoD Instruction 5200.40, "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

(f) NDP-1, "National Disclosure Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 1, 1988

(g) Management Initiative Decision (MID) 912, "Joint Battle Management Command and Control," January 7, 2003[2]

---

[2] This reference is FOR OFFICIAL USE ONLY and release is restricted to authorized organizations.

# E2. ENCLOSURE 2

## DEFINITIONS

E2.1.1. Combined Enterprise Regional Information Exchange System (CENTRIXS). The DoD multinational information sharing portion of the GIG. CENTRIXS is a standing, global enterprise network allowing the United States and coalition nations and their forces, in a seamless manner, to securely share operational and intelligence information in support of combined planning, a unity of effort and decision superiority in multinational operations.

E2.1.2. Community of Interest (COI). The ability, from a single workstation, to have secure, dynamic, information exchanges with multiple, separate networks.

E2.1.3. Enterprise Network. Designated by the DoD CIO Executive Board as Enterprise Networks for providing a defined capability, serving multiple DoD Components, remaining cognizant with the GIG architecture, abiding management with Enterprise-wide oversight, and providing service to any user with a validated requirement.

E2.1.4. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (d)). The GIG supports the Department of Defense, the National Security Agency, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

E2.1.5. MNIS CENTRIXS. Includes the CENTRIXS, the GRIFFIN (Globally Reaching Interactive Fully Functional Information Network), the CFBL (Combined Federated Battle Lab), and other MNIS network programs, as well as related cross-domain security programs associated with the sharing of information with foreign nations and forces, as an integrated MNIS solution to support the combined warfighting environment.