



Department of Defense **INSTRUCTION**

NUMBER 8410.02
December 19, 2008

ASD(NII)/DoD CIO

SUBJECT: NetOps for the Global Information Grid (GIG)

References: See Enclosure 1

1. PURPOSE. This Instruction, issued under the authority of DoD Directive (DoDD) 5144.1 (Reference (a)):

- a. Incorporates and cancels DoD Chief Information Officer (CIO) Guidance and Policy Memorandums No. 10-8460 and No. 4-8460 (References (b) and (c)).
- b. Establishes policy and assigns responsibilities for implementing and executing NetOps, the DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG.
- c. Institutionalizes NetOps as an integral part of the GIG.

2. APPLICABILITY. This Instruction applies to:

- a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint 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 within the Department of Defense (hereafter referred to collectively as the "DoD Components").
- b. All GIG information systems; associated processes, personnel, and technology; and GIG interfaces to DoD mission partners.
- c. DoD-owned and controlled information systems operated by a contractor or other entity on behalf of the Department of Defense that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. NetOps shall be instituted and conducted to support DoD missions, functions, and operations in a manner that enables authorized users and their mission partners to access and share timely and trusted information on the GIG from any location at any time, to the maximum extent allowed by law and DoD policy.

b. NetOps is the responsibility of all DoD Components. Per the Unified Command Plan (Reference (d)), the mission is assigned to the Commander, U.S. Strategic Command (CDRUSSTRATCOM), to plan, integrate, and coordinate DoD global network operations by directing GIG operations and defense.

c. GIG Enterprise Management (GEM), GIG Net Assurance (GNA), and GIG Content Management (GCM) functions shall be operationally and technically integrated to ensure simultaneous and effective monitoring, management, and security of the enterprise.

d. As information systems capabilities mature, they shall be capable of reporting their system status to include fault, configuration, performance, and security to facilitate GIG health and mission readiness assessments.

e. NetOps-related data shall be shared and exchanged through common interoperable standards in accordance with DoD net-centric data strategy.

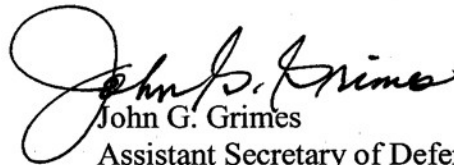
f. A common set of NetOps mission-driven metrics, measurements, and reporting criteria shall be used to assess GIG operating performance and to determine the mission impact of service degradations or outages.

g. NetOps requirements shall be addressed and incorporated in doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF).

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This Instruction is effective immediately.



John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration /
DoD Chief Information Officer

Enclosures

1. References
 2. Responsibilities
- Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
- (b) DoD Chief Information Officer Guidance and Policy Memorandum No. 10-8460, "GIG Network Operations," August 24, 2000 (hereby canceled)
- (c) DoD Chief Information Officer Guidance and Policy Memorandum No. 4-8460, "GIG Networks," August 24, 2000 (hereby canceled)
- (d) "Unified Command Plan," May 5, 2006¹
- (e) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (f) DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001
- (g) Secretary of Defense Memorandum, "Assignment and Delegation Authority to Director, Defense Information Systems Agency (DISA)," June 18, 2004
- (h) DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006
- (i) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (j) Memorandum of Agreement Between the Assistant Secretary of Defense for Networks and Information Integration and the Intelligence Community (IC) Chief Information Officer for "Sharing Network Management and Computer Network Defense Information," June 24, 2005²
- (k) DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense,"
December 2, 2004
- (l) Secretary of Defense Memorandum, "Forces for Unified Commands-FY 2006 (U),"
February 15, 2006
- (m) DoD Directive S-5100.44, "Defense and National Leadership Command Capability
(DNLCC) (U)," July 9, 2008
- (n) DoD Directive 3020.26, "Defense Continuity Program (DCP)," September 8, 2004
- (o) DoD 5200.1-R, "Information Security Program," January 14, 1997
- (p) USD(I) memorandum, "Interim Information Security Guidance," April 16, 2004
- (q) GIG Architecture Federation Strategy, August 2007²
- (r) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology
(IT) and National Security Systems (NSS)," May 5, 2004
- (s) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated
Terms," as amended
- (t) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation
Process (DIACAP)," November 28, 2007

¹ Requests for copies can be forwarded to the Director for Strategic Plans and Policy, J-5/Joint Staff, and will be provided in accordance with laws, regulations, and policies concerning the treatment of FOUO information.

² Requests for copies can be forwarded to the Director for Computing and NetOps, OASD(NII) DoD CIO, and will be provided in accordance with laws, regulations, and policies concerning the treatment of unclassified information.

ENCLOSURE 2

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO, in addition to the responsibilities in paragraph 6 of this enclosure, shall:

a. Provide strategy, policy, oversight, and guidance for NetOps across the DoD Enterprise in accordance with Reference (a).

b. Ensure that capabilities for operating and defending the GIG are acquired in coordination with the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) and are managed, integrated, and synchronized consistent with Reference (a).

c. Establish necessary agreements with applicable non-DoD and non-U.S. agencies, organizations, mission partners, allies, and coalition partners to facilitate NetOps pursuant to Reference (a).

d. In coordination with the Under Secretary of Defense for Intelligence (USD(I)), provide policy guidance to the Director, National Security Agency, regarding NetOps and operational aspects of information assurance, as described in DoDD 8500.01E and DoDD O-8530.1 (References (e) and (f)).

e. Develop NetOps capability increments in collaboration with functional owners and Capability Portfolio Managers to ensure efficient and secure GIG operations.

f. Enforce implementation of approved DoD IT policy.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). The Director, DISA, under the authority, direction, and control of the ASD(NII)/DoD CIO, shall, in addition to the responsibilities specified in paragraph 6 of this enclosure and Secretary of Defense Memorandum (Reference (g)) and in accordance with DoDD 5105.19 (Reference (h)), provide and maintain the minimum essential set of technical standards, specifications, and interfaces, including naming conventions, required for the development and use of interoperable capabilities.

3. USD(AT&L). The USD(AT&L), in coordination with the ASD(NII)/DoD CIO and in addition to the responsibilities in paragraph 6 of this enclosure, shall provide direction and guidance concerning the acquisition of NetOps capabilities.

4. USD(I). The USD(I), in addition to the responsibilities in paragraph 6 of this enclosure, shall:

a. Serve as the DoD focal point to the Intelligence Community (IC) for all NetOps policy and oversight matters relating to intelligence information sharing and interoperability of Defense intelligence systems and processes in accordance with DoDD 5143.01 (Reference (i)).

b. Require the Director, Defense Intelligence Agency (DIA), as the manager of the sensitive compartmented information (SCI) component of the GIG, to interact with the Director of National Intelligence (DNI) and facilitate coordination and sharing of DoD SCI network status and situational awareness (SA) information in accordance with the Memorandum of Agreement (MOA) between the ASD(NII)/DoD CIO and the IC CIO (Reference (j)).

5. DIRECTOR, OPERATIONAL TEST AND EVALUATION (DOT&E). The DOT&E, in coordination with the ASD(NII)/DoD CIO, USD(AT&L), Chairman of the Joint Chiefs of Staff, and CDRUSSTRATCOM and in addition to the responsibilities in paragraph 6 of this enclosure, shall:

a. Ensure processes, procedures, and infrastructure are available to operationally test and evaluate NetOps capabilities that are developed and acquired.

b. Conduct periodic assessments of NetOps processes, procedures, and capabilities as part of the DOT&E-led assessments.

6. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Execute NetOps functions within DoD Component-operated portions of the GIG in accordance with Reference (g) and in support of Combatant Commanders' responsibilities defined in paragraphs 8 and 9 of this enclosure.

b. Plan, procure, develop, test, and implement capabilities for operating and defending the GIG that are consistent with DoD policy and strategic guidance.

c. Ensure personnel are trained, equipped, resourced, and forces organized to implement and execute NetOps. Ensure DOTMLPF is consistent with this policy.

d. Share GIG SA data with Combatant Commands, other DoD Components and the IC and in accordance with DoDD 8320.02 (Reference (k)).

e. Establish and provide the necessary resources to ensure compliance with service level agreements and MOAs among GIG service providers and customers.

f. Participate in the NetOps community of interest (COI) to share information, promote standards, and resolve NetOps issues.

g. Participate in the enterprise architecture (EA) efforts described in paragraph 9.h. of this enclosure.

h. Ensure that all DoD contractors and other entities operating DoD-owned information systems and DoD-controlled information systems on behalf of the Department of Defense that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, comply with this Instruction.

7. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities specified in paragraph 6 of this enclosure, shall:

a. In coordination with the ASD(NII)/DoD CIO, provide direction and guidance concerning the integration and development of NetOps-related capabilities in the Joint Capabilities Integration and Development System process, including directing the appropriate changes to achieve target NetOps capability increments and ensuring that the Combatant Commands' enterprise architectures address existing and future NetOps capabilities requirements.

b. In coordination with the Combatant Commanders, identify NetOps capabilities needed to support joint, combined, coalition, and other operations with mission partners.

c. Develop and coordinate joint NetOps policies, guidance, and instructions.

d. Incorporate NetOps into joint doctrine.

8. COMMANDERS OF THE COMBATANT COMMANDS. The Commanders of the Combatant Commands, in addition to the responsibilities specified in paragraph 6 of this enclosure, shall:

a. Direct GIG operations and defense consistent with functional or geographic responsibilities and in coordination with CDRUSSTRATCOM.

b. Identify NetOps requirements for supporting DoD Components and DoD mission partners. Serve as a focal point for NetOps with coalition partners.

c. Retain authority to approve or deny DoD Component-initiated GIG modifications with theater and/or global impacts.

9. CDRUSSTRATCOM. The CDRUSSTRATCOM, in addition to the responsibilities specified in paragraphs 6 and 8 of this enclosure, shall:

a. Direct GIG operations and defense in accordance with Reference (d) and through assigned forces as listed in Secretary of Defense Memorandum (Reference (l)). In coordination with other

Combatant Commanders and other DoD Components, develop and implement a command and control structure to execute NetOps operational priorities.

b. Identify and advocate NetOps characteristics and capabilities in consultation with ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, and the other Heads of the DoD Components.

c. Coordinate intelligence and information sharing activities involving DoD SCI networks with the IC Incident Response Center in accordance with the established procedures approved by the Secretary of Defense and the DNI or their designees pursuant to Reference (j).

d. Advise the Chairman of the Joint Chiefs of Staff on NetOps-related matters affecting National Military Command System performance, the integrity of the GIG, or actions needed to support DoD operations as described in DoDD S-5100.44 (Reference (m)).

e. Coordinate with the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, and the other Heads of the DoD Components to develop and implement a NetOps continuity of operations capability per DoDD 3020.26 (Reference (n)).

f. In coordination with Commander, U.S. Joint Forces Command (CDRUSJFCOM), sponsor and conduct periodic joint training and exercises to assess NetOps procedures, capabilities, and effects.

g. Establish criteria for classifying NetOps and GIG SA information in accordance with DoD 5200.1-R and USD(I) memorandum (References (o) and (p)).

h. In coordination with the Director, DISA, and the other Heads of the DoD Components, lead the development of the required operational views for a NetOps EA in compliance with the GIG Architecture Federation Strategy (Reference (q)) to ensure interoperability and capability needs are addressed in accordance with DoDD 4630.05 (Reference (r)).

i. Establish a NetOps COI to provide a forum to share information, promote standards, and resolve NetOps issues. The NetOps COI shall develop and publish a standard set of NetOps metrics, measurements, and processes to enable consistent enterprise-wide monitoring and assessment of GIG health, security, and mission readiness.

j. In coordination with the Heads of the DoD Components, develop and publish a comprehensive DoD NetOps data strategy and implementation plan in accordance with Reference (k).

k. Identify to all DoD Components the minimum SA information required to operate and defend the GIG.

10. CDRUSJFCOM. The CDRUSJFCOM, in addition to the responsibilities specified in paragraphs 6 and 8 of this enclosure, and in coordination with the CDRUSSTRATCOM, shall:

a. Conduct joint experiments and exercises to develop and refine NetOps procedures and requirements.

b. Oversee and synchronize joint NetOps training to ensure commonality and compatibility among the DoD Components.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CDRUSJFCOM	Commander, U.S. Joint Forces Command
CDRUSSTRATCOM	Commander, U.S. Strategic Command
CIO	Chief Information Officer
COI	community of interest
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DOT&E	Director, Operational Test and Evaluation
DoDD	Department of Defense Directive
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
EA	enterprise architecture
GCM	GIG Content Management
GEM	GIG Enterprise Management
GIG	Global Information Grid
GNA	GIG Net Assurance
IC	Intelligence Community
MOA	Memorandum of Agreement
SA	situational awareness
SCI	sensitive compartmented information
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this Directive.

continuity of operations. Defined in Joint Publication 1-02 (Reference (s)).

DoD-controlled information systems. Defined in DoD Instruction 8510.01 (Reference (t)).

EA. A strategic information asset base that defines the mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. EA includes a baseline architecture, a target architecture, and a sequencing (transition) plan.

GCM. The set NetOps functions that ensures information is available on the GIG by enabling users to safeguard, compile, catalog, discover, cache, distribute, retrieve, and share data in a collaborative environment.

GEM. The set NetOps functions that encompasses the GIG's information technology services management. These consist of the many elements and processes needed to communicate across the full spectrum of the GIG, to include enterprise services management, systems management, network management, satellite communications management, and electromagnetic spectrum management.

GIG SA. The ability to acquire and share information across and external to the GIG in a manner that enables users, operators, and commanders to attain timely and accurate, shared understanding of the health, security, and mission readiness of the GIG in order to proactively operate and defend the GIG in support of current, planned, and potential future operations.

GNA. The set NetOps functions that includes the operational responsibilities for information assurance, computer network defense (to include computer network defense response actions), and critical infrastructure protection in defense of the GIG.

information system. Defined in Reference (s).

mission partners. Non-DoD individuals and organizations that support or are supported by DoD missions and operations. Mission partners include allies, coalition partners, host nations, international and multinational organizations, civilian government agencies and departments (Federal, State, local, and tribal), law enforcement agencies, non-governmental agencies and organizations (private volunteer organizations, commercial businesses, academic institutions, etc.), and other non-adversaries.

NetOps. The DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG. NetOps includes, but is not limited to, enterprise management, net assurance, and content management. NetOps provides commanders with GIG situational awareness to make informed command and control decisions. GIG situational awareness is gained through the operational and technical integration of enterprise management and defense actions and activities across all levels of command (strategic, operational, and tactical).