



Department of Defense

DIRECTIVE

NUMBER 3020.40

January 14, 2010

Incorporating Change 2, September 21, 2012

USD(P)

SUBJECT: DoD Policy and Responsibilities for Critical Infrastructure

References: See Enclosure 1

1. PURPOSE. This Directive:

a. Updates, renames, and reissues DoD Directive (DoDD) 3020.40 (Reference (a)) to assign responsibilities for the Defense Critical Infrastructure Program (DCIP).

b. Establishes policy and assigns responsibilities for the execution of roles assigned to the Department of Defense pursuant to Homeland Security Presidential Directive 7 and DoD Instruction 5220.22 (References (b) and (c)), and ensures consistency with applicable provisions of the National Infrastructure Protection Plan (Reference (d)) and compliance with applicable provisions of part 29 of title 6, Code of Federal Regulations (Reference (e)).

c. Implements Reference (b), which assigns critical infrastructure and/or key resource (CI/KR) responsibilities to the Department of Defense.

d. Designates the Defense Infrastructure Sector Lead Agents (DISLAs) and assigns their specific roles and responsibilities.

2. APPLICABILITY

a. This Directive applies to:

(1) 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 in the Department of Defense (hereafter referred to collectively as the "DoD Components").

(2) The DISLAs identified in section 15 of Enclosure 2 of this Directive.

b. Nothing herein shall be interpreted to subsume or replace the responsibilities, functions, or authorities of the OSD Principal Staff Assistants (PSAs), the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, or the Heads of the Defense Agencies or of the DoD Field Activities as prescribed by law or DoD guidance.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Coordination on the risk management of defense critical infrastructure (DCI) shall be accomplished with other Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries, as appropriate.

b. DCI risk management actions shall:

(1) Be coordinated and accomplished by responsible authorities.

(2) Support incident management.

(3) Protect DCI-related sensitive information.

c. The DCIP shall coequally complement and not be subordinate to other DoD programs, functions, and activities that contribute to mission assurance through risk management.

d. The DCIP shall:

(1) Determine the risks to DCI.

(2) Implement DoD-wide procedures to respond to risks to DCI and work with other Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries, as appropriate.

(3) Support and advocate for initiatives to respond to risks to national critical infrastructure as appropriate and within DoD legal authorities.

e. DCIP activities related to the defense industrial base (DIB) shall be consistent with and executed pursuant to the authorities established by Reference (c).

f. Information on DCIP plans, programs, and assets shall be protected in accordance with pertinent DoD issuances on information and operations security and, only as applicable, in accordance with Reference (e) and its implementing Department of Homeland Security (DHS) issuances.

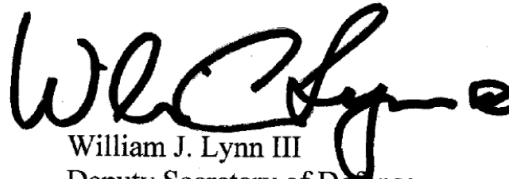
5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Directive 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 directive:

a. Is effective January 14, 2010.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (f)). If not, it will expire effective January 14, 2020 and be removed from the DoD Issuances Website.



William J. Lynn III
Deputy Secretary of Defense

Enclosures

1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005 (hereby canceled)
- (b) Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003
- (c) DoD Instruction 5220.22, "National Industrial Security Program," March 18, 2011
- (d) Department of Homeland Security, "National Infrastructure Protection Plan (NIPP)," 2009
- (e) Part 29 of title 6, Code of Federal Regulations
- (f) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
- (g) Sections 131-134 of title 6, United States Code
- (h) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008
- (i) DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
- (j) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
- (k) National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008¹
- (l) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002
- (m) DoD Directive 5101.11E, "DoD Executive Agent for the Military Postal Service (MPS) and Official Mail Program (OMP)," June 2, 2011
- (n) Section 11103 of title 40, United States Code
- (o) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002

¹ Copies of this restricted distribution document are available to authorized personnel upon request to DHS.

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P), in addition to the responsibilities in section 8 of this enclosure, shall:

a. Serve as the PSA to the Secretary of Defense on the risk management of DCI.

b. Establish and oversee the implementation of DCIP policy and guidance for the risk management of DCI, including issuance of strategies, plans, and standards. Review DoD Component and DISLA implementation plans referenced in paragraph 9.b. of this enclosure.

c. Establish policy for promoting DCIP information sharing with other Federal departments and agencies; State, local, regional, territorial, and tribal entities; intergovernmental organizations (IGOs) and nongovernmental organizations (NGOs); the private sector; and foreign countries while safeguarding information from disclosure that could harm DoD operations or that could jeopardize information safeguarding agreements with DCIP stakeholders.

d. Manage the assigned sector-specific agency responsibilities for the national DIB Sector on behalf of the Secretary of Defense.

(1) Coordinate matters pertaining to the DIB with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); the Under Secretary of Defense for Intelligence (USD(I)); and the DoD Chief Information Officer (DoD CIO).

(2) Consult with appropriate Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries on matters pertaining to the DIB.

e. Serve as the principal DoD representative for DCIP-related matters with Congress; the Executive Office of the President; other Federal departments and agencies; State, local, regional, territorial, and tribal entities; IGOs and NGOs; the private sector; foreign countries; and other entities, including the national DIB Sector Government Coordinating Council (GCC), the DIB Critical Infrastructure Partnership Advisory Council (CIPAC), and other national-level partnership mechanisms established by References (b) and (d). Review appropriate non-DoD policy for DCIP equities.

f. Develop and implement, in coordination with the DoD CIO and the Chairman of the Joint Chiefs of Staff, a DCIP net-centric approach to information sharing. Ensure that the DCIP enterprise architecture promotes DCIP interoperability of information systems and processes with the DHS-established national infrastructure enterprise architecture, and that it supports business needs and facilitates decision making by the DoD Components and the DISLAs.

g. Develop, implement, and oversee, in accordance with the DHS-established Protected Critical Infrastructure Information (PCII) Program and DCIP requirements, a DoD PCII Program to facilitate the sharing of critical infrastructure information voluntarily provided by private sector entities pursuant to sections 131-134 of title 6, United States Code (U.S.C.) (Reference (g)).

h. Consolidate DoD Component and DISLA intelligence production requirements related to critical infrastructure responsibilities and provide them to the USD(I). In coordination with the USD(I), the Secretaries of the Military Departments, and the Chairman of the Joint Chiefs of Staff, ensure the timely dissemination of DCI-related threat and hazard assessments and warnings, as appropriate, to the DoD Components, the DISLAs, and other authorized activities. Ensure the USD(I) receives information reflecting the viability and security of DCI operating under the National Industrial Security Program (NISP), pursuant to Reference (c).

i. Oversee risk management activities, including monitoring and reporting, related to DoD-owned DCI with priority emphasis on defense critical assets. For non-DoD-owned DCI, oversee the management, within DoD, of risks to mission execution (including passing gathered risk-related data to appropriate DoD officials) and work, as appropriate, with other Federal departments and agencies; State, local, regional, territorial, and tribal entities; IGOs; NGOs; the private sector; and foreign countries to encourage and support risk management efforts at these assets.

j. In coordination with the Chairman of the Joint Chiefs of Staff, develop guidance for and ensure the implementation of DCIP education, training, and outreach activities.

k. Integrate all DoD Component and DISLA requirements and priorities for risk management of DCI.

l. Coordinate DoD collaborative efforts with DHS in the national-level sector partnership organizations established by References (b) and (d).

m. Coordinate inclusion of appropriate DCI in the Infrastructure Data Warehouse maintained by DHS, subject to security constraints.

n. Appoint DoD Co-Chairs of the national DIB Sector GCC and the DIB CIPAC.

o. Provide a DoD PCII Officer to oversee the PCII Program within the Department of Defense in accordance with Reference (e).

p. Lead the DoD effort, supported by appropriate DoD Components and the DISLAs, to collaborate with partners in the private sector; other Federal departments and agencies; State, local, regional, territorial, and tribal entities; GCCs, IGOs, and NGOs; and foreign countries to:

(1) Identify and prioritize all non-DoD-owned DCI (including all DIB facilities) using established criteria.

(2) Encourage risk management strategies to mitigate the impact of attacks against, or the consequences of catastrophic failures of, all non-DoD-owned DCI (including all DIB facilities).

q. Assign DoD representatives to these national sector GCCs: Chemical; Nuclear Reactor, Materials, and Waste; Emergency Services; and National Monuments and Icons.

r. Coordinate and integrate activities with other DoD risk management programs and activities, to include organizational policies, guidance, plans, and orders as they relate to DCI.

s. Coordinate with the DoD CIO on DIB cyber security and information assurance (CS/IA) activities to protect unclassified DoD information requiring controls pursuant to DoD Instruction 5200.1, DoD Manual 5200.01, Volume 4, and DoDD 5230.09 (References (h) through (j)) that transits or resides on DIB systems and networks.

t. Support other DoD missions related to critical infrastructure that are assigned to the Secretary of Defense in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (k)).

u. Provide guidance to; monitor the activities of; and review, validate, and advocate funding for the DISLA for the Space Sector identified in paragraph 15.a. of this enclosure. Coordinate such matters with the Secretary of the Air Force and the Chairman of the Joint Chiefs of Staff.

2. USD(AT&L). The USD(AT&L), in addition to the responsibilities in section 8 of this enclosure and with the support of the USD(P), shall:

a. Integrate DCIP policies into acquisition, procurement, military construction, and installation guidance. Ensure DCIP-related guidance is developed and implemented that requires that, prior to system fielding or deployment, either commercial system developers remediate or the appropriate senior-level DoD program manager documents a risk management decision for all vulnerabilities identified.

b. In coordination with the USD(P), develop policies, make recommendations, provide guidance, and approve science and technology efforts related to DCI. Synchronize these efforts with DHS science and technology efforts where appropriate.

c. Identify vulnerabilities in technologies relied upon by DCI that are developed, acquired, owned, or operated by the Department of Defense, and develop effective risk response options to emerging vulnerabilities or threats to include cyber threats.

d. Provide guidance to; monitor the activities of; and review, validate, and advocate funding for the DISLAs identified in paragraph 15.a. of this enclosure for the DIB, Logistics, Public Works, and Transportation Sectors. Coordinate such matters with the USD(P) and the Chairman of the Joint Chiefs of Staff, as appropriate.

e. Assign DoD representatives to the national Critical Manufacturing, Energy, Government Facilities, and Transportation Sector GCCs as appropriate.

f. Provide representatives to the national DIB Sector GCC as appropriate.

g. Oversee the DISLA for the DIB Sector in conducting an annual review of criteria for the identification and prioritization of DIB assets critical to execution of DoD missions. Oversee the DISLA's application of the criteria to assets across the DIB and provide the resulting DIB Critical Asset List to the USD(P).

h. As the OSD PSA overseeing the performance of the DoD Executive Agent for DoD postal activities pursuant to DoDDs 5101.1 and 5101.11E (References (l) and (m)), assign DoD representatives to the national Postal and Shipping Sector GCC, as appropriate.

i. Identify, develop, update, and implement policy and processes into the DoD acquisition contracting process for improved protection of unclassified DoD information regarding controls required by References (h) through (j) on unclassified DIB systems and networks as part of DIB CS/IA activities.

3. USD(I). The USD(I), in addition to the responsibilities in section 8 of this enclosure and in coordination with the USD(P), shall:

a. Designate the Defense Infrastructure Sector Critical Infrastructure Assurance Officer (CIAO) for the Intelligence Sector as the primary intelligence advisor for the DCIP. Direct the Intelligence Sector CIAO to plan, integrate, coordinate, direct, synchronize, and manage all aspects of intelligence support for the DCIP.

b. Establish policy and oversee intelligence, counterintelligence, and security support to the DCIP and, as appropriate, the national DIB Sector GCC, including DCI operating under the NISP, pursuant to Reference (c).

c. Establish intelligence collection policy for DCIP and DIB national sector efforts. Ensure through appropriate procedural dialogue that DCIP and national DIB Sector intelligence requirements are reflected in Combatant Command, Military Department, DoD, and national collection plans.

d. Establish policy for sharing and maintaining DCIP and national sector-related threat assessments and, in coordination with the USD(P) and the Chairman of the Joint Chiefs of Staff, establish DCIP intelligence production priorities.

e. Provide guidance to; monitor the activities of; and review, validate, and advocate funding for the DISLA for the Intelligence Sector identified in paragraph 15.a. of this enclosure. Coordinate such matters with the USD(P) and the Chairman of the Joint Chiefs of Staff, as appropriate.

f. Provide representatives to the national DIB Sector GCC.

4. UNDER SECRETARY OF DEFENSE (COMPTROLLER) (USD(C)/CHIEF FINANCIAL OFFICER (CFO), DEPARTMENT OF DEFENSE. The USD(C)/CFO, in addition to the responsibilities in section 8 of this enclosure and with the support of the USD(P), shall:

a. Provide guidance to the DoD Components and the DISLAs for displaying DCIP-related resourcing within budget submissions.

b. Provide guidance to; monitor the activities of; and review, validate, and advocate funding for the DISLA for the Financial Services Sector identified in paragraph 15.a. of this enclosure. Coordinate such matters with the USD(P) and the Chairman of the Joint Chiefs of Staff, as appropriate.

c. Assign DoD representatives to the national Banking and Finance Sector GCC, as appropriate.

5. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R), in addition to the responsibilities in section 8 of this enclosure and with the support of the USD(P), shall:

a. Develop policy to ensure the integration of the Reserve Components in the risk management of DCI within the United States and its territories, in coordination with the USD(P), the Secretaries of the Military Departments, and the Chairman of the Joint Chiefs of Staff.

b. Provide guidance to; monitor the activities of; and review, validate, and advocate funding for the DISLA for the Personnel Sector. Coordinate such matters with the USD(P) and the Chairman of the Joint Chiefs of Staff, as appropriate.

c. Provide guidance to, monitor the activities of, and review, advocate, and advise on DISLA funding for the Health Affairs Sector with the assistance of the Assistant Secretary of Defense for Health Affairs (ASD(HA)). Coordinate such matters with the USD(P) and the Chairman of the Joint Chiefs of Staff, as appropriate.

d. Assign DoD representatives to the national Food and Agriculture Sector and the Public Health and Healthcare Sector GCCs, as appropriate.

e. Develop policy and plans to implement readiness reporting requirements for DCI.

6. ASD(HA). The ASD(HA), under the authority, direction, and control of USD(P&R), shall assist and advise the USD(P&R) on DISLA funding for the Health Affairs Sector as required.

7. DoD CIO. The DoD CIO, in addition to the responsibilities in section 8 of this enclosure, shall:

a. Coordinate with the USD(P) on integrating DIB CS/IA activities into DCIP.

b. Oversee and advise the USD(P) on CS/IA initiatives related to the DCIP within the DoD Components and the DISLAs using established IA and IA-enabled information technology products and coordinate CS activities to include the sharing of cyber-related vulnerability data and best practices with other Federal departments and agencies; State, local, regional, territorial, and tribal entities; and foreign countries, as appropriate.

c. Provide guidance to; monitor the activities of; and review, validate, and advocate funding for the DISLA for the Global Information Grid (GIG) Sector identified in paragraph 15.a. of this enclosure. Coordinate such matters with the USD(P) and the Chairman of the Joint Chiefs of Staff, as appropriate.

d. Assign DoD representatives to the national Communications and Information Technology Sector GCCs, as appropriate.

e. Provide a representative to the national DIB Sector GCC.

f. Support the USD(P) in promoting DCIP interoperability of information systems and processes including interoperability of all DCIP-related information systems, applications, and databases with the DHS-established national infrastructure enterprise architecture, subject to security constraints.

g. Provide expertise to the USD(P) in developing policy for sharing information concerning DCIP matters with Congress; the Executive Office of the President; other Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; foreign countries; and other foreign entities, including the national-level partnership mechanisms established by References (b) and (d).

8. USD(AT&L), USD(I), USD(C)/CFO, USD(P&R), DoD CIO, AND USD(P). The USD(AT&L), USD(I), USD(C)/CFO, USD(P&R), DoD CIO, and USD(P) shall:

a. Integrate DCIP requirements into programs within their purview.

b. Support collaboration and information sharing between national-level sector infrastructure protection planning, mitigation, and remediation efforts and the corresponding defense infrastructure sector, where applicable.

9. HEADS OF THE DoD COMPONENTS, DISLAs, AND CHIEF, NATIONAL GUARD BUREAU (NGB). The Heads of the DoD Components, the DISLAs, and the Chief, NGB, in support of their assigned critical infrastructure responsibilities, as appropriate, shall:

a. Establish an office of primary responsibility with the capability to implement and execute DCIP program requirements and to develop, communicate, and maintain up to and including TOP SECRET sensitive compartmented information DCI-related data.

b. Develop, publish, and maintain comprehensive DCIP implementation plans that shall include program vision and end state, program goals and objectives, major program milestones, major functional responsibilities and program capabilities, dissemination and/or sharing of program outputs, and results that support the overall DCIP execution.

c. Coordinate and integrate activities with other DoD risk management programs and activities, and integrate DCIP policies and activities into organizational policies, guidance, plans, and orders as they relate to DCI. Incorporate DCIP policies into contracts, as appropriate.

d. Establish the necessary lines of communication and promote information sharing with each other and with Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries, as appropriate.

e. Provide, maintain, and review critical infrastructure risk management data, as appropriate.

f. Coordinate or consult, as appropriate, with the necessary DoD Components; DISLAs; Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries to implement a standardized process for DCI and inter- and intra-dependency identification based upon assigned DoD missions. Develop, maintain, and share a list of their organization DCI, as appropriate.

g. Monitor and report DCI-related threat and hazard assessments and changes. Annually provide to the USD(P) their intelligence production requirements for implementing DCIP responsibilities through appropriate reporting chains.

h. Annually nominate recommendations to the Chairman of the Joint Chiefs of Staff for, and monitor the results of, DCI vulnerability assessments; risk assessments; risk response actions; and additions, changes, or deletions to the DCI list.

i. Identify, validate, and submit consolidated and prioritized resource requirements to the appropriate authority.

j. Participate in the Planning, Programming, Budgeting, and Execution System, as well as other related resource and prioritization processes (e.g., unfunded resource requests, Integrated Priority List), and provide adequate DCIP resources in their baseline budgets to support and enable program capabilities, objectives, and priorities as appropriate.

k. Provide, as directed, to the USD(P) through appropriate reporting chains, their respective organization's DCIP program implementation status and resourcing data.

l. Develop and implement procedures to respond to DCI-related emergencies and exercises. Collect and provide DCI-related information and recommendations to appropriate decision makers.

m. Conduct DCIP education, outreach, and training activities in accordance with published education and outreach goals, objectives, and standards.

10. SECRETARIES OF THE MILITARY DEPARTMENTS; COMMANDER, U.S. SPECIAL OPERATIONS COMMAND (CDRUSSOCOM); CHIEF, NGB; AND DIRECTORS OF THE DEFENSE AGENCIES AND DoD FIELD ACTIVITIES. In addition to the responsibilities in section 9 of this enclosure, the Secretaries of the Military Departments; CDRUSSOCOM; Chief, NGB (in coordination with the National Guard Adjutants General of the States, as appropriate); and the Directors of the Defense Agencies and the DoD Field Activities shall:

a. Incorporate requirements for the risk management of DCI in acquisition, maintenance, and sustainment contracts, as well as in facility construction, installation recapitalization, and installation-level outsourcing and privatization efforts.

b. Collect and disseminate DCI-related threat and hazard assessments and warnings, as appropriate, to subordinate elements, the DoD Components, the DISLAs, and other authorized activities.

c. With the support of the appropriate DoD Components and DISLAs, conduct assessments of the threat and hazards, vulnerability, and risk to DoD-owned DCI and the inter- and intra-dependencies needed to accomplish required DoD missions. Document and provide the results to the appropriate DoD Components and DISLAs.

d. With the support of the appropriate DoD Components and DISLAs, document a risk decision for all DoD-owned DCI, including a risk response plan if appropriate. Provide a risk decision and risk reduction plan to the appropriate DoD Components and DISLAs.

e. Act to manage the risk of loss or degradation of DCI. Coordinate with the Commanders of the Combatant Commands, the Chairman of the Joint Chiefs of Staff, and the USD(P) to identify and integrate their priorities for remediation and mitigation of DCI. Program resources as appropriate to implement DCIP risk management decisions.

f. Incorporate DCIP into education, outreach, and training programs, including the testing and exercising of mitigation and response plans.

11. SECRETARY OF THE ARMY. The Secretary of the Army, in addition to the responsibilities in sections 8 and 9 of this enclosure, shall direct the Commander, U.S. Army

Corps of Engineers, to assign DoD representatives to the national Dams Sector and Water Sector GCCs, as appropriate.

12. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities in section 9 of this enclosure, shall:

a. Serve as the principal military advisor to the Secretary of Defense on the risk management of DCI.

b. Coordinate with the DoD Components and the DISLAs to provide an integrated set of DCIP priorities for DCI vulnerability assessment, risk assessment, and risk response to the appropriate Military Departments, Defense Agencies, and/or the U.S. Special Operations Command for action, and to the other DoD Components and the DISLAs for situational awareness.

c. Integrate DCIP functions and activities into joint planning, doctrine, training, and exercises; assist the USD(P) in the development and maintenance of DCIP standards and procedures.

d. Review Combatant Command DCIP-related doctrine, standards, procedures, training, implementation plans, and program status reports.

e. Assess the capability of the Combatant Commands, Military Departments, and Defense Agencies to monitor and report all relevant DCIP-related data on threats, hazards, vulnerabilities, and related trends, and assist the USD(I) and the USD(P) in implementing processes for monitoring, reporting, and sharing DCIP-related threat information.

f. Oversee the development of DCIP processes and procedures, including the nomination, scheduling, and execution of risk- and vulnerability-based assessment programs. Maintain a catalog of vulnerability assessments related to DCI. Provide an annual report to the USD(P) on DCIP implementation throughout the Department of Defense.

13. COMMANDERS OF THE COMBATANT COMMANDS. The Commanders of the Combatant Commands, through the Chairman of the Joint Chiefs of Staff, in addition to the responsibilities in section 9 of this enclosure, shall:

a. In coordination with the DoD asset owner, the Heads of the other DoD Components, and the DISLAs, act to prevent or mitigate the loss or degradation of DoD-owned DCI within their assigned areas of responsibility.

b. For non-DoD-owned DCI within their assigned areas of responsibility, in coordination with the Chairman of the Joint Chiefs of Staff and the USD(P), act to prevent or mitigate the loss or degradation of DCI only at the direction of the Secretary of Defense, with the exception of responding to a sudden and unexpected event where only military forces are able to prevent

significant damage to mission-critical infrastructure, and where circumstances preclude obtaining prior authorization from the Secretary of Defense or the President. Promptly report any action taken to the National Military Command Center.

c. Capture intelligence collection requirements pertinent to DCIP in Combatant Command intelligence collection plans.

d. Collect, analyze, and evaluate threat and hazard incidents and/or events and disseminate necessary advisories and warnings to the DoD Components, the DISLAs, other authorized activities, and subordinates.

14. CHIEF, NGB. The Chief, NGB, in addition to the responsibilities in sections 9 and 10 of this enclosure, shall provide a representative to the national DIB Sector GCC.

15. DISLAs. The DISLAs, in addition to the responsibilities in section 9 of this enclosure, shall:

a. Be assigned the defense infrastructure sector shown in the Table.

Table. DISLA Assignments

<u>DEFENSE INFRASTRUCTURE SECTOR</u>	<u>LEAD AGENT</u>
DIB	Director, Defense Contract Management Agency
Financial Services	Director, Defense Finance and Accounting Service
GIG	Director, Defense Information Systems Agency
Health Affairs	ASD(HA)
Intelligence	Director, Defense Intelligence Agency
Logistics	Director, Defense Logistics Agency
Personnel	Director, DoD Human Resources Activity
Public Works	Chief, U.S. Army Corps of Engineers
Space	Commander, U.S. Strategic Command
Transportation	Commander, U.S. Transportation Command

b. Assign a general or flag officer or a member of the Senior Executive Service to serve as their respective Defense Infrastructure Sector CIAO.

c. Establish and maintain a characterization of their defense infrastructure sector functions, systems, assets, and dependencies as they relate to supporting DoD operational capabilities and assets.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HA)	Assistant Secretary of Defense for Health Affairs
CDRUSSOCOM	Commander, United States Special Operations Command
CI/KR	critical infrastructure and/or key resource
CIAO	Critical Infrastructure Assurance Officer
CIPAC	Critical Infrastructure Partnership Advisory Council
CS	cyber security
DCI	defense critical infrastructure
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DIB	defense industrial base
DISLA	Defense Infrastructure Sector Lead Agent
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
GCC	Government Coordinating Council
GIG	Global Information Grid
IA	information assurance
IGO	intergovernmental organization
NGB	National Guard Bureau
NGO	nongovernmental organization
NISP	National Industrial Security Program
PCII	Protected Critical Infrastructure Information
PSA	Principal Staff Assistant
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USG	U.S. Government

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Directive:

asset. A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations.

characterization. The analytic decomposition of functions, systems, assets, and dependencies related to supporting DoD operational capabilities and assets.

CS. Includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster.

DCI. The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. DCI is a combination of task critical assets and defense critical assets.

DCIP. A DoD risk management program that seeks to ensure the availability of DCI.

defense critical asset. An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions.

defense infrastructure sector. A virtual association within the DCIP that traverses normal organizational boundaries and encompasses defense networks, assets, and associated dependencies that perform similar functions within the Department of Defense and are essential to the execution of the National Defense Strategy. The defense infrastructure sectors are:

DIB Sector. The DoD, U.S. Government (USG), and private sector worldwide industrial complex with capabilities to perform research, development, and design and to produce and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

Financial Services Sector. The DoD, USG, and private sector worldwide network and its supporting infrastructure that meet the financial services needs of the Department of Defense across the range of military operations.

GIG Sector. 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. It includes all owned and leased communications (commercial telecommunication infrastructure) 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 11103 of title 40, U.S.C. (Reference (n)).

Health Affairs Sector. The DoD, USG, and private sector worldwide healthcare network and its supporting infrastructure that meet the healthcare needs of DoD personnel across the range of military operations.

Intelligence Sector. Those DoD, USG, and private sector facilities, networks, and systems (assets) located worldwide or extra-terrestrially that conduct and support the collection, production, and dissemination of intelligence, surveillance, and reconnaissance information essential to the execution of the National Military Strategy. These assets encompass human intelligence, geospatial intelligence, measurement and signature intelligence, signals intelligence, open-source intelligence, and technical intelligence; counterintelligence collection, processing, and exploitation means; and all-source analysis and production, including the networks and means over which intelligence information is shared, communicated, and/or disseminated.

Logistics Sector. The DoD, USG, and private sector worldwide facilities, networks, and systems that support the provision of supplies and services to U.S. forces.

Personnel Sector. The DoD, USG, and private sector worldwide network that coordinates and supports personnel and human resource functions of DoD personnel.

Public Works Sector. The DoD, USG, and private sector worldwide network, including the real property inventories (environment, land, buildings, and utilities), that manages the support, generation, production, and transport of commodities (e.g., electric power, oil and natural gas, water and sewer, and emergency services) for and to the Department of Defense.

Space Sector. The DoD, USG, and private sector worldwide network, including both space- and ground-based systems and facilities, that supports launch, operation, maintenance, specialized logistics, and control systems for the space assets relied upon by the Department of Defense.

Transportation Sector. The DoD, USG, and private sector worldwide network that provides military lift support (surface, sea, and air) for U.S. military operations.

dependency. A relationship or connection in which one entity is influenced or controlled by another entity.

DISLAs. Designated DoD officials and their respective defense sector organizations that perform defense infrastructure sector responsibilities. In coordination with their respective PSAs, the DISLAs characterize their defense infrastructure sectors to identify functions, systems, interdependencies, and, ultimately, sector task critical assets that support Combatant Command, Military Department, and Defense Agency missions and sector functions.

GCC. Defined in Reference (d).

hazards. Non-hostile incidents such as accidents, natural forces, and technological failure that cause loss or damage to infrastructure assets.

IGO. An organization comprised primarily of sovereign states (referred to as member states), or of other IGOs.

information assurance. Defined in DoDD 8500.01E (Reference (o)).

infrastructure. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole.

inter-dependency. Relationships or connections between entities of different DoD Components and defense infrastructure sectors.

intra-dependency. Relationships or connections between entities of a DoD Component and a defense infrastructure sector.

mission assurance. A process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the execution of DoD mission-essential functions in any operating environment or condition.

mitigation. Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure.

national infrastructure sector. One of the 18 national CI/KR sectors identified in Reference (b).

network. A group or system of interconnected or cooperating entities, normally characterized as being nodes (assets), and the connections that link them.

NGO. A legally-constituted organization created by persons having the legal authority to do so with no participation or representation of any government.

remediation. Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified.

risk. Probability and severity of loss linked to threats or hazards and vulnerabilities.

risk assessment. A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.

risk management. A process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits.

risk response. Actions taken to remediate or mitigate risk, or to reconstitute capability in the event of loss or degradation.

sector-specific agency. Federal departments and agencies identified in Reference (b) as responsible for CI/KR protection activities in specified national CI/KR sectors.

task critical asset. An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD Components or DISLA organizations to execute the task or mission-essential task it supports. Task critical assets are used to identify defense critical assets.

threat. An adversary having the intent, capability, and opportunity to cause loss or damage.

vulnerability. A weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

vulnerability assessment. A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities.