# Department of Defense
# DIRECTIVE

**NUMBER** 3020.40
August 19, 2005

ASD(HD)

SUBJECT: Defense Critical Infrastructure Program (DCIP)

References: (a) DoD Directive 5160.54, "Critical Asset Assurance Program," January 20, 1998 (hereby canceled)
(b) Homeland Security Presidential Directive #7, December 17, 2003
(c) Deputy Secretary of Defense Memorandum, "Critical Infrastructure Protection Responsibilities and Realignments," August 11, 1999 (hereby canceled)
(d) The Department of Defense Critical Infrastructure Protection Plan, November 18, 1998 (hereby superceded)
(e) through (g), see enclosure 1

## 1. PURPOSE

1.1. This Directive cancels reference (a), updates policy, and assigns responsibilities for the Defense Critical Infrastructure Program (DCIP), incorporating guidance from the President in reference (b) to function as the Sector-Specific Agency for the Defense Industrial Base (DIB) with the following responsibilities:

1.1.1. Collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector.

1.1.2. Conduct or facilitate vulnerability assessments of the sector.

1.1.3. Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

1.2. This Directive cancels reference (c) and supersedes reference (d) and the Deputy Secretary of Defense memorandum dated September 3, 2003 (reference (e)).

## 2. APPLICABILITY AND SCOPE

2.1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, 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").

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

## 3. DEFINITIONS

3.1. Defense Critical Infrastructure. DoD and non-DoD networked assets essential to project, support, and sustain military forces and operations worldwide.

3.2. Defense Critical Infrastructure Program (DCIP). A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.

3.3. Additional terms used in this Directive are defined in enclosure 1.

## 4. POLICY

It is DoD policy that:

4.1. Defense Critical Infrastructure, which includes DoD and non-DoD domestic and foreign infrastructures essential to planning, mobilizing, deploying, executing, and sustaining U.S. military operations on a global basis, shall be available when required. Coordination on remediation and/or mitigation shall be accomplished with other Federal Agencies, State and local governments, the private sector, and equivalent foreign entities, as appropriate.

4.2. Vulnerabilities found in Defense Critical Infrastructure shall be remediated and/or mitigated based on risk management decisions made by responsible authorities.

4.3. The identification, prioritization, assessment, and assurance of Defense Critical Infrastructure shall be managed as a comprehensive program that includes the development of adaptive plans and procedures to mitigate risk, restore capability in the event of loss or

degradation, support incident management, and protect Defense Critical Infrastructure related sensitive information.

4.4. The DCIP shall complement other DoD programs and efforts, such as: force protection; antiterrorism; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness – all of which contribute to mission assurance.

4.5. DCIP activities related to the Defense Industrial Base (DIB) shall be consistent with and executed by those authorities responsible for the National Industrial Security Program (NISP). DCIP DIB efforts shall utilize the NISP (DoD Directive 5220.22, reference (f)) to the maximum extent practical.

4.6. Information on DCIP plans, programs, and assets shall be safeguarded in accordance with pertinent DoD issuances on information and operations security.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Homeland Defense (ASD(HD)), under the Under Secretary of Defense for Policy (USD(P)), shall:

5.1.1. Serve as the principal civilian advisor to the Secretary of Defense on the identification, prioritization, and protection of Defense Critical Infrastructure, including providing advice on the readiness of and risks to Defense Critical Infrastructure and the adequacy of resources to execute the National Military Strategy.

5.1.2. Develop and ensure the implementation of DCIP policy and program guidance for the identification, prioritization, and protection of Defense Critical Infrastructure including issuance of strategies and standards.

5.1.3. Assist the Secretary of Defense in his role as the lead Sector-Specific Federal Agency Official for the DIB. Coordinate matters pertaining to the DIB with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)).

5.1.4. Serve as the principal DoD representative for DCIP-related matters with the Congress, the Executive Office of the President, other Federal Agencies, State and local entities, the public, host nations, and other foreign entities.

5.1.5. In coordination with the Under Secretary of Defense for Intelligence and the Chairman of the Joint Chiefs of Staff ensure the timely dissemination of DCIP-related vulnerability and threat assessments and warnings, as appropriate, to the DoD Components and other authorized activities.

5.1.6. Develop policy for promoting information sharing while safeguarding information from disclosure that could harm DoD operations or could jeopardize information safeguarding agreements with DCIP stakeholders.

5.1.7. Develop and implement a DCIP enterprise architecture to ensure a net-centric approach to promote DCIP interoperability of information systems and processes, support business needs, and facilitate critical decision making by DoD Components in coordination with the Assistant Secretary of Defense for Networks and Information Integration and the Chairman of the Joint Chiefs of Staff.

5.1.8. Ensure the implementation of DCIP education, training, and awareness activities in coordination with the Chairman of the Joint Chiefs of Staff.

5.1.9. Integrate all DoD Component DCIP requirements and priorities for critical assets and related vulnerabilities.

5.2. The Assistant Secretary of Defense for International Security Policy (ASD(ISP)), under the USD(P), shall provide guidance to and monitor the activities of the Defense Sector Lead Agency for Space identified in subparagraph 5.11.1. and coordinate such matters with the ASD(HD), the Secretary of the Air Force, and the Chairman of the Joint Chiefs of Staff.

5.3. The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the USD(P), shall:

5.3.1. Integrate DCIP policies into acquisition, procurement, and installation policy guidance.

5.3.2. Identify vulnerabilities in technologies relied upon by DoD critical infrastructure that are developed, acquired, owned, or operated by the DoD, and develop effective countermeasures to emerging vulnerabilities or threats.

5.3.3. Coordinate with the ASD(HD) to develop policies, make recommendations, issue guidance, and approve science and technology (S&T) efforts related to the DCIP.

5.3.4. Coordinate with the ASD(HD) to ensure DCIP-related guidance is developed and implemented, requiring that system providers remediate vulnerabilities identified prior to system fielding or deployment.

5.3.5. Provide guidance to and monitor the activities of the Defense Sector Lead Agencies identified in subparagraph 5.11.1. for DIB, Logistics, Public Works, and Transportation. Coordinate such matters with the ASD(HD) and the Chairman of the Joint Chiefs of Staff, as appropriate.

5.4. The Under Secretary of Defense for Intelligence (USD(I)), in coordination with the USD(P), shall:

5.4.1. Establish policy to provide intelligence, counterintelligence, and security support to the DCIP.

5.4.2. Establish intelligence collection policy for DCIP-efforts, establish policy for sharing and maintaining DCIP-related threat assessments, and in coordination with the ASD(HD) and the Chairman of the Joint Chiefs of Staff, validate DCIP intelligence collection priorities.

5.4.3. Provide guidance to and monitor the activities of the Defense Sector Lead Agency for Intelligence, Surveillance, and Reconnaissance (ISR) identified in subparagraph 5.11.1. Coordinate such matters with the ASD(HD) and the Chairman of the Joint Chiefs of Staff, as appropriate.

5.5. The Under Secretary of Defense (Comptroller)/Chief Financial Officer (USD(C)/CFO), in coordination with the USD(P), shall:

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

5.5.2. Provide guidance to and monitor the activities of the Defense Sector Lead Agency for Financial Services identified in subparagraph 5.11.1. in coordination with the ASD(HD).

5.6. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)), in coordination with the USD(P), shall:

5.6.1. In coordination with the ASD(HD) and the Chairman of the Joint Chiefs of Staff, develop policy to ensure integration of the Reserve components and the National Guard Bureau in the identification, prioritization, and protection of Defense Critical Infrastructure within the United States and its territories.

5.6.2. Provide guidance and monitor the activities of the Defense Sector Lead Agencies for Health Affairs and Personnel identified in subparagraph 5.11.1. in coordination with the ASD(HD).

5.7. The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) shall:

5.7.1. Provide guidance to and monitor the activities of the Defense Sector Lead Agency for the Global Information Grid (GIG) identified in subparagraph 5.11.1. in coordination with the ASD(HD) and the Chairman of the Joint Chiefs of Staff, as appropriate.

5.7.2. Ensure, through the Defense-Wide Information Assurance (IA) Program (DIAP), the coordination of IA initiatives with the DoD Components through established IA and IA-enabled information technology products used in assuring the integrity, availability, confidentiality, authentication, and non-repudiation of DCIP-related information.

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

5.8.1. Serve as the principal military advisor to the Secretary of Defense on the identification, prioritization, and protection of Defense Critical Infrastructure including advice on the readiness of and risks to Defense Critical Infrastructure.

5.8.2. Identify an office of primary responsibility for DCIP activities.

5.8.3. Submit to the Military Departments an integrated set of Combatant Command DCIP priorities for mitigation, remediation, readiness, and risk management plans.

5.8.4. Validate and prioritize Combatant Commands and their respective component command mission essential tasks, related capabilities, critical asset assessment recommendations, and identified vulnerabilities related to the DCIP.

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

5.8.6. Review DCIP-related doctrine, standards, procedures, and training of Combatant Commands and Military Departments.

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

5.8.8. Implement a vulnerability assessment program in accordance with DCIP guidance and standards.

5.9. The Commanders of Combatant Commands within their respective regional or functional areas of responsibility shall:

5.9.1. Identify an office of primary responsibility to establish, resource, and execute a command program for matters pertaining to the identification, prioritization, and protection of Defense Critical Infrastructure, including the identification and prioritization of Command mission essential tasks and required capabilities. Identify, validate, prioritize, and submit resource requirements in accordance with established Planning, Programming, Budgeting and Execution process procedures, and advise the Chairman of the Joint Chiefs of Staff of the resource requirements necessary to achieve DCIP objectives.

5.9.2. Coordinate with the Military Departments, the Defense Agencies, DoD Field Activities, and Defense Sector Lead Agencies identified in subparagraph 5.11.1., to identify and assess critical assets and associated infrastructure interdependencies pertinent to mission accomplishment within assigned regional or functional areas of responsibility.

5.9.3. Act to prevent or mitigate the loss or degradation of DoD-owned critical assets within assigned regional or functional areas of responsibility. For non-DoD-owned critical assets within assigned regional or functional areas of responsibility, act to prevent or mitigate the loss or degradation only at the direction of the Secretary of Defense and in coordination with the Chairman of the Joint Chiefs of Staff and the ASD(HD), with the exception of responding to a time critical event that would require specific actions by military forces to prevent significant damage to mission-critical infrastructure.

5.10. The Secretaries of the Military Departments, the Commander, U.S. Special Operations Command, the Chief, National Guard Bureau (in coordination with the National Guard Adjutants General of the States), and the Directors of Defense Agencies and DoD Field Activities shall:

5.10.1. Identify an office of primary responsibility for matters pertaining to the identification, prioritization, and protection of Defense Critical Infrastructure. Establish, resource, and execute an organizational program supporting the DCIP.

5.10.2. Identify and prioritize mission essential tasks and required capabilities within areas in which they perform missions and over which they have responsibility.

5.10.3. Identify, assess, and document, in coordination with other DoD Components and Defense Sector Lead Agencies identified in subparagraph 5.11.1., critical assets and associated infrastructure dependencies needed to implement required Combatant Command capabilities and other statutory responsibilities.

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

5.10.5. Incorporate requirements for the identification, prioritization, and protection of Defense Critical Infrastructure in acquisition, maintenance, and sustainment contracts; and in facility construction, installation recapitalization, and installation-level outsourcing and privatization efforts.

5.10.6. Collect and disseminate DCIP-related threat assessments and warnings, as appropriate, to subordinate elements, other DoD Components, and other authorized activities. Program resources as appropriate to implement DCIP risk management recommendations.

5.10.7. In coordination with the Commanders of the Combatant Commands, the Chairman of the Joint Chiefs of Staff, and the ASD(HD), act to prevent or mitigate loss or degradation of critical assets.

5.11. Defense Critical Infrastructure Program Defense Sector Lead Agents shall:

5.11.1. Be hereby assigned as follows:

| DEFENSE SECTOR | LEAD AGENT |
|---|---|
| Defense Industrial Base (DIB) | Director, Defense Contract Management Agency |
| Financial Services | Director, Defense Finance & Accounting Service |
| Global Information Grid (GIG) | Director, Defense Information Systems Agency |
| Health Affairs | Assistant Secretary of Defense for Health Affairs |
| Intelligence, Surveillance, and Reconnaissance (ISR) | 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 |

5.11.2. Assign a Senior Executive/Flag Officer to serve as the Defense Sector Critical Infrastructure Assurance Officer, and identify an office of primary responsibility for matters pertaining to the identification, prioritization, and protection of Defense Critical Infrastructure. Establish, resource, and execute a program supporting the DCIP in assigned defense sectors, including the development and coordination of a Defense Sector Assurance Plan.

5.11.3. Establish and maintain a characterization of the Defense Sector support functions, systems, assets, and dependencies as they relate to operational capabilities and assets identified by the DoD Components.

5.11.4. Collaborate with other Defense Sector Lead Agencies and DoD Components to identify cross-sector interdependencies.

5.11.5. Plan and coordinate with all DoD Components that own or operate elements of the Defense Sector to identify, analyze, and assess the Defense Sector's critical assets and related mission impacts.

6. EFFECTIVE DATE

This Directive is effective immediately.

Gordon England
Acting Deputy Secretary of Defense

Enclosures – 2
E1. References, continued
E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) Deputy Secretary of Defense Memorandum, "Realignment of Critical Infrastructure Protection Oversight to the Assistant Secretary of Defense for Homeland Defense," September 3, 2003 (hereby superceded)
(f) DoD Directive 5220.22, "DoD Industrial Security Program," September 27, 2004
(g) Section 1401(2) of title 40, United States Code

# E2. ENCLOSURE 2

## DEFINITIONS[1]

E2.1.1. Asset (Infrastructure). A distinguishable network entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and owned or operated by domestic, foreign, public, or private sector organizations.

E2.1.2. Characterization (Infrastructure). The analytic decomposition of functions, systems, assets, and dependencies as they relate to supporting DoD operational capabilities and assets.

E2.1.3. Critical Infrastructure Protection (CIP). Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc.

E2.1.4. Defense Critical Asset. An asset of such extraordinary importance to DoD 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.

E2.1.5. Defense Critical Infrastructure. DoD and non-DoD networked assets essential to project, support, and sustain military forces and operations worldwide.

E2.1.6. Defense Critical Infrastructure Program (DCIP). A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.

E2.1.7. Defense Industrial Base (DIB) Defense Sector. The Department of Defense, the U.S. Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

E2.1.8. Defense Sector. A virtual association within the DCIP that traverses normal organizational boundaries, 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 Military Strategy.

E2.1.9. Dependency. A relationship or connection whereby one entity is influenced or controlled by another entity:

[1] The terms defined in this enclosure are to be forwarded to the Chairman of the Joint Chiefs of Staff for inclusion or revisions of terms in the JCS Pub 1-02

E2.1.9.1. Inter-Dependency. Relationships or connections between entities of different functions, networks, sectors, or services.

E2.1.9.2. Intra-Dependency. Relationships or connections between entities within a common function, network, sector, or service.

E2.1.10. Financial Services Defense Sector. The DoD, government, and private sector worldwide network and its supporting infrastructure that meet the financial services needs of DoD users across the range of military operations.

E2.1.11. Global Information Grid (GIG) Defense 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 including 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 (g)).

E2.1.12. Hazard (Infrastructure). Non-hostile incidents such as accidents, natural forces, technological failure, etc., that cause loss or damage to infrastructure assets.

E2.1.13. Health Affairs Defense Sector. The DoD, government and private sector worldwide health care network and its supporting infrastructure that meet the health care needs of DoD users across the range of military operations.

E2.1.14. Infrastructure. The framework of networked assets that comprise identifiable industries, institutions, or distribution capabilities that enable a continued flow of goods and services.

E2.1.15. Installation Preparedness. The integration of key activities on DoD installations and facilities that address all efforts pertaining to prevention, detection, protection, response, and remediation against all threats and hazards.

E2.1.16. Intelligence, Surveillance, and Reconnaissance (ISR) Defense Sector. The DoD, government and private sector worldwide facilities, networks, and systems that conduct and support the collection, production, and dissemination of intelligence, surveillance and reconnaissance information, in support of activities that meet the needs of DoD users across the range of military operations.

E2.1.17. Logistics Defense Sector. The DoD, government, and private sector worldwide facilities, networks, and systems that support the provision of supplies and services to U.S. forces.

E2.1.18. Mission Assurance. A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy. It links numerous risk management program activities and security related functions—such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—to create the synergistic effect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.

E2.1.19. 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.

E2.20. Monitoring and Reporting. The collection, fusion, and dissemination of intelligence-based indications and warning, DoD asset and civil infrastructure readiness reporting, law enforcement information, man-made or natural hazards, and suspicious security event reporting, that can adversely impact mission readiness.

E2.1.21. Network. A group or system of interconnected or cooperating entities, normally characterized as being nodes (assets) and the connections that link them.

E2.22. Personnel Defense Sector. The DoD, government, and private sector worldwide network that coordinates and supports personnel and human resource functions of DoD personnel.

E2.1.23. Public Works Defense Sector. The DoD, government, 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, emergency services, etc.) for and to DoD users.

E2.1.24. Remediation. Actions taken to correct known deficiencies and weaknesses. These actions are undertaken once a vulnerability has been identified.

E2.1.25. Risk. Probability and severity of loss linked to threats or hazards.

E2.1.25.1. Risk Assessment. A systematic examination of risk, using disciplined processes, methods, and tools. It provides an environment for decision making to continuously evaluate and prioritize risks and recommend strategies to remediate or mitigate those risks.

E2.1.25.2. Risk Management. A process by which decision makers accept, reduce, or offset risk.

E2.1.26. Space Defense Sector. The DoD, government, and private sector worldwide network, including both space- and ground-based systems and facilities, that supports launch, operation, maintenance, specialized logistics, control systems, etc., for DoD users.

E2.1.27. Threat. An adversary having the intent, capability, and opportunity to cause loss or damage.

E2.1.28. Transportation Defense Sector. The DoD, government, and private sector worldwide network that provides U.S. military lift support (surface, sea, and air) for military operations.

E2.1.29. Vulnerability (Infrastructure). The characteristics 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.

E2.1.30.Vulnerability Assessment (Infrastructure). A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities.