



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, D.C. 20350-1000

SECNAVINST 3501.1D
DUSN (P)
22 Jan 2018

SECNAV INSTRUCTION 3501.1D

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Ref: See Enclosure (1).

Encl: (1) References
(2) Responsibilities
(3) Risk Management
(4) Acronyms and Definitions

1. Purpose

a. This instruction implements the Department of the Navy (DON) Critical Infrastructure Protection (CIP) Program per references (a) through (n) and establishes DON CIP policy and processes that align with the Department of Defense (DoD) Mission Assurance Strategy, per reference (o). The DON CIP Program assures the availability of assets and infrastructure that are critical to planning, mobilizing, deploying, executing, and sustaining core DON capabilities, missions, and military operations.

b. Significant changes found in this revision include updated organizational responsibilities (enclosure (2)) and risk management guidance (enclosure (3)), and the appointment of the Deputy Under Secretary of the Navy for Policy (DUSN (P)) as DON Office of Primary Responsibility (OPR) for the CIP Program, per reference (a).

2. Cancellation. SECNAVINST 3501.1C

3. Definitions. See enclosure (4).

4. Applicability and Scope. This instruction applies to the Office of the Secretary of the Navy (SECNAV); the Chief of Naval Operations (CNO); the Commandant of the Marine Corps (CMC); all U.S. Navy and U.S. Marine Corps installations, commands,

activities, and field offices; and all other organizational entities within the DON.

5. Policy. It is DON policy to:

a. Strengthen the protection and resilience of its critical infrastructure against manmade and naturally occurring threats and hazards. Such critical infrastructure enables continued execution of DON capabilities, Mission Essential Tasks (MET), and Mission Essential Functions (MEF). The DON and its Military Services shall work together to proactively manage and reduce risk that has potential to impact mission execution. These efforts shall seek to identify and disrupt threats, reduce vulnerabilities, and minimize consequences while retaining the flexibility and agility necessary to plan for and respond to future protection needs. When loss or degradation of critical infrastructure occurs, plans shall be implemented to minimize impacts and restore mission capability. Priority shall be given to DON Defense Critical Assets (DCA), Tier I task critical assets (TCA), and Tier II TCAs, respectively.

b. Synchronize the CIP Program with other DON programs, activities, and security-related functions, per reference (o), that contribute to the risk management of critical infrastructure. Applicable programs, activities, and functions include: Antiterrorism; Force Protection; Continuity of Operations; Cybersecurity; Emergency Management; Physical Security; Chemical, Biological, Radiological, and Nuclear Defense; Counterintelligence and Law Enforcement; and energy resilience.

c. Implement the CIP Program per references (a) through (n). References (h) through (n) and enclosure (3) provide policy and guidance for the identification, assessment, and management of risk to critical infrastructure within the DoD and DON.

d. Require the DON Critical Infrastructure Assurance Officer (CIAO) and Navy and Marine Corps CIP leads to maintain the ability to store, handle, and share Defense Critical Infrastructure Program (DCIP) information up to and including Top Secret (Sensitive Compartmented Information) (TS (SCI)). Other designated DON CIP Program personnel shall maintain the ability to store, handle, and share DCIP information

commensurate to the highest level required to perform CIP duties.

6. Responsibilities. See enclosure (2).

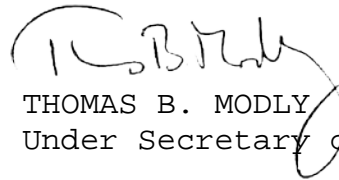
7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of January 2012. Applicable retention requirements may be found under the following SSICs in SECNAV M-5210.1, Part III: 3057, 3058, 3440, 3010.4, 4700, 11000, 11014, 11090, and 11100.

8. Reports Control. The reporting requirements contained in this instruction are exempt from reports control per Part IV of SECNAV M-5214.1 of December 2005. The specific exemptions are applied as follows:

a. Paragraphs 3a(1)(a) and 3c(2) of enclosure (2) of this instruction are exempt per SECNAV M-5214.1, Part IV, paragraphs 7e and 7k.

b. Paragraph 5b(1) of Enclosure (2) of this instruction is exempt per SECNAV M-5214.1, Part IV, paragraph 7k.

c. Paragraph 11c of Enclosure (2) of this instruction is exempt per SECNAV M-5214.1, Part IV, paragraphs 7c and 7o.



THOMAS B. MODLY

Under Secretary of the Navy

Distribution:

Electronic only, via DON Issuances Web site

<http://doni.documentservices.dla.mil>

REFERENCES

- (a) Under Secretary of the Navy Memorandum, Department of the Navy Critical Infrastructure Protection Program of 1 February 2016
- (b) 10 U.S.C., Armed Forces
- (c) SECNAVINST 5430.7R, Assignment of Responsibilities and Authorities in the Officer of the Secretary of the Navy
- (d) National Security Strategy of February 2015
- (e) E.O. 13636, Improving Critical Infrastructure Cybersecurity
- (f) Presidential Policy Directive 21 of 12 February 2013
- (g) The National Military Strategy of the United States of America of February 2015
- (h) DoD Directive 3020.40, Mission Assurance (MA) of 29 November 2016
- (i) DoD Instruction 3020.45, Defense Critical Infrastructure Program (DCIP) Management of 21 April 2008
- (j) DoDM 3020.45, Volume 1, Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP) of 24 October 2008
- (k) DoDM 3020.45, Volume 2, Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning of 28 October 2008
- (l) DoDM 3020.45, Volume 3, CH 1, Defense Critical Infrastructure Program (DCIP): Security Classification Manual (SCM) of 15 February 2011
- (m) DoDM 3020.45, Volume 5, CH 1, Defense Critical Infrastructure Program (DCIP): Execution Timeline of 23 May 2017
- (n) DoD Instruction 5240.19, Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP) of 31 January 2014
- (o) DoD Mission Assurance Strategy of 7 May 2012
- (p) SECNAVINST 5500.36, Department of the Navy Security Enterprise
- (q) SECNAVINST 5000.2E, Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System
- (r) SECNAVINST 5430.107, Mission and Functions of the Naval Criminal Investigative Service
- (s) DoD Instruction 2000.16, Department of Defense Antiterrorism Standards of 17 November 2016
- (t) DoD Instruction 6055.17: Department of Defense Emergency Management (EM) Program of 13 February 2017

RESPONSIBILITIES

1. The Under Secretary of the Navy (UNSECNAV), is designated as the deputy and principal assistant to the SECNAV, and acts with the full authority of SECNAV in managing the DON, per reference (b). Per reference (c), UNSECNAV oversees DON critical infrastructure.

2. DUSN (P) shall:

a. Serve as the DON CIAO and the office of primary responsibility for DON CIP Program policy, oversight, and advocacy.

b. Serve as the Senior Executive responsible for DON Security enterprise management, accountability and oversight decisions, and make security-related resource recommendations to the SECNAV per reference (p).

c. Develop, publish, and maintain comprehensive DON CIP Program policy and guidance.

3. The DUSN (P) Senior Director for Security shall:

a. Serve as the DON Deputy CIAO and oversee the DON CIP Program policy implementation.

(1) Conduct periodic reviews of Navy and Marine Corps CIP programs, including:

(a) Review risk management of DON DCAs and Tier I TCAs, e.g., assessment reports, risk management decisions.

(b) Observe Navy and Marine Corps assessments of critical assets.

(2) Conduct periodic reviews of Secretariat-level organizations performing CIP functions.

b. Convene a DON CIP working group at least quarterly, to coordinate DON CIP efforts among stakeholders.

c. Provide appropriate representation to the Office of the Assistant Secretary of Defense for Homeland Defense and Global

Security (OASD (HD&GS)) and other federal agencies for matters pertaining to CIP policy, oversight, and resource advocacy. Examples include, but are not limited to:

(1) Reviewing and coordinating DoD and other federal CIP policy. Coordinate with, compile, and adjudicate responses from the Secretariat, Navy, and Marine Corps, and develop a single DON position on their behalf.

(2) Providing consolidated oversight reports to OASD (HD&GS) as requested. Coordinate with and compile data from the Secretariat, Navy, and Marine Corps to fulfill this responsibility.

(3) Forwarding DON DCA points of contact information to the OASD (HD&GS).

(4) Notifying OASD (HD&GS) of any event that degrades or destroys a DCA and the resulting impact on DON, Navy, and Marine Corps missions.

d. Collaborate with the DCIP community to establish the requirements to maintain and share DCIP data and documentation to an authoritative database. This includes advocating for a database that:

(1) Provides for secure storage of DON CIP-related classified data and documents up to and including TS (SCI).

(2) Is fully interoperable with existing Navy and Marine Corps databases, and the DCIP community where appropriate.

(3) Includes functionality to capture, monitor, and share critical asset risk reduction planning and implementation efforts.

e. Coordinate with the Office of the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)) to ensure that requirements for the risk management of Defense Critical Infrastructure (DCI) are identified for incorporation into acquisition, maintenance, and sustainment contracts per references (h) and (q).

4. The DON SE EXCOM is responsible for providing senior-level leadership, program oversight, and guidance to the DON CIP Program. As required, the DON SE EXCOM shall provide direction and recommendations regarding the governance, implementation, and execution of DON and Service CIP policy.

a. Members of the DON SE EXCOM shall additionally:

(1) Foster CIP Program cooperation and collaboration within the DON, DoD, and other federal organizations to improve program effectiveness.

(2) Institutionalize CIP policy throughout the DON and direct appropriate actions to support Navy and Marine Corps efforts in ensuring mission assurance for the Combatant Commands (CCMD) in the execution of reference (p).

(3) Ensure that policies within their areas of responsibility, which may be affected by CIP policy, are revised as necessary to integrate CIP factors and requirements into associated programs and activities.

5. The DON CIP Program Working Group is responsible for program policy implementation and execution feedback. Working Group membership is comprised of subject matter experts at grades O-5/O-6 or civilian equivalents from all organizations listed within this enclosure. Members additionally participate as DON representatives to their respective Defense Infrastructure Sectors.

a. The Working Group will be chaired by the DON Deputy CIAO and shall convene at least quarterly to support DON CIP Program initiatives as provided in reference (a) through (s).

b. Members of the Working Group shall support of DON CIP oversight, participate in the program review process conducted by the DON CIAO, in accordance with this policy and references (h) through (s).

6. The DON Chief Information Officer shall, as the DON's senior official for Information Management, Information Technology, and matters involving Cybersecurity:

a. Appoint a DON representative to the Defense Infrastructure Sector for the DoD Information Network.

b. Appoint a subject matter expert(s), knowledgeable in Information Management and Information Technology matters, as the DON Chief Information Officer representative(s) to the DON CIP Program Working Group.

7. The ASN (RD&A) shall:

a. Appoint a subject matter expert(s), knowledgeable in acquisition, Defense Industrial Base (DIB), logistics, transportation, and space matters, as the ASN (RD&A) representative(s) to the DON CIP Program Working Group and as the DON representative(s) to the Defense Infrastructure Sectors for DIB, Logistics, Transportation, and Space.

b. Work with the DON CIAO and Service CIP representatives to identify, characterize, prioritize, and remediate vulnerabilities to critical infrastructures and processes managed by the acquisition community.

c. Review policies related to or affected by CIP and revise as necessary, as directed by references (h) and (q).

d. Require CIP policy consideration in contracts and acquisition management procedures by incorporating requirements for the identification, prioritization, and protection of DCI in the maintenance, sustainment, and life cycles of acquisition programs.

8. The Assistant Secretary of the Navy for Manpower and Reserve Affairs (ASN (M&RA)) shall:

a. Appoint a personnel subject matter expert as the ASN (M&RA) representative to the DON CIP Program Working Group and as the DON representative to the Defense Infrastructure Sector for Personnel.

b. Coordinate and provide Secretariat-level support to the Services' procedures for remediating and mitigating risks associated with mission essential personnel operations

9. The Assistant Secretary of the Navy for Financial Management and Comptroller (ASN (FM&C)) shall:

a. Appoint a financial subject matter expert as the ASN (FM&C) representative to the DON CIP Program Working Group and as the DON representative to the Defense Infrastructure Sector for Financial Services, per reference (h).

b. Coordinate and provide Secretariat-level support to the Services' procedures for remediating and mitigating risks associated with mission essential financial operations.

10. The Assistant Secretary of the Navy for Energy, Installations, and Environment (ASN (EI&E)) shall:

a. Appoint a subject matter expert(s), knowledgeable in public works, environmental, and energy matters, as the ASN (EI&E) representative(s) to the DON CIP Program Working Group and as the DON representative(s) to the Defense Infrastructure Sector for Public Works.

b. Advocate for CIP-related programmatic and budgetary expenditures.

c. Coordinate and provide Secretariat-level support to the Services' AT and CIP programs to ensure:

(1) Energy and environmental activities and requirements are factored into risk assessments.

(2) Energy-related infrastructure that could severely impact DON missions is protected.

d. Monitor Navy and Marine Corps critical infrastructure remediation and mitigation efforts.

e. Coordinate with the DON CIAO and other DoD Components and Agencies to develop information sharing initiatives.

f. Ensure that CIP policy is considered in the review of plans and policies, including those concerning privatization and public-private ventures; make CIP policy an integral factor in directing ASN (EI&E) actions relating to facilities and

utilities planning, energy security, design, construction, and maintenance.

11. The Director, Naval Criminal Investigative Service (NCIS) shall:

a. Appoint a subject matter expert(s), knowledgeable in the areas of vulnerability and risk assessments as well as indications and warning, as the NCIS representative(s) to the DON CIP Program Working Group and as the DON representative(s) to the Defense Infrastructure Sector for Intelligence.

b. Provide comprehensive and timely reporting of foreign intelligence entity threats, incidents, events, and trends to DCIP authorities and the DoD Components for CIP per reference (r) and in consonance with the Office of Naval Intelligence and the DUSN (P) Intelligence Directorate. Provide threat information directly to commands and owners charged with protection of affected critical infrastructure; and upon request, copy the DON CIAO and Service CIP points of contact for awareness.

c. Provide DCIP focused counterintelligence support to the DON and the Defense Infrastructure Sector Lead Agents (DISLA) per reference (n). This coverage shall include, but not be limited to, providing threat and vulnerability assessments for DCI owned by the DON or a DoD affiliated organization tasked to NCIS. The information shall be provided to DON installation commanders, and upon request, the DON CIAO, and Service CIP points of contact.

d. Prepare and provide validated counterintelligence products annually as required in order to carry out CIP responsibilities on Navy or Marine Corps owned DCI to be monitored for threats per reference (h).

e. Upon request, assist Service CIP points of contact in the identification of vulnerabilities to critical infrastructure and assets and in the development of remediation strategies.

12. The Surgeon General/Chief Bureau of Medicine and Surgery (BUMED) shall appoint a subject matter expert, knowledgeable in the area of health related threats and vulnerabilities, as the BUMED representative to the DON CIP Program Working Group and as

the DON representative to the Defense Infrastructure Sector for Health Affairs.

13. General Counsel of the Navy (GC). The GC shall:

- a. Appoint a representative at the DON CIP working group.
- b. Provide legal advise and counsel, as necessary or requested, to the DON CIP working group as an advisor.

14. The CNO and the CMC shall execute DON CIP policy and assign offices of primary responsibility within their respective Services to:

- a. Develop and maintain a Service-level CIP Program, formalized in policy, to ensure the identification, prioritization, assessment, management of risk, and protection of critical assets and associated infrastructure per this instruction and references (h) through (m).

- b. Establish an "all threats and hazards" risk assessment/risk management process, per guidance provided in Enclosure (3). This process is designed to:

- c. Establish a process to disseminate DCI related threat assessment and hazard warnings to installation commanders, CIP points of contact, and mission and asset owners.

- d. Identify, validate, prioritize, assess, and manage risk to DON critical assets and infrastructure.

- (1) Coordinate the Critical Asset Identification Process with applicable DON CIP stakeholders, including DON CIP Program Working Group members.

- (2) Document and maintain a list of critical assets and associated supporting infrastructure dependencies, per references (h) and (j), in an authoritative database and ensure the database is accessible to the DCIP community.

- (3) Ensure critical assets are assessed, including the parameters of criticality, vulnerabilities, and associated threats and hazards, to determine risk of loss, per references (h), (i) and (s).

(a) Annually, nominate critical assets and infrastructure for DCI risk assessments, per references (h) and (m). Include the name of the organization that will conduct the assessment and an organization point of contact.

(b) Coordinate with CCMDs, the Joint Staff, and Defense Infrastructure Sectors, as needed, to identify and schedule critical assets and infrastructure to be assessed by existing and future processes.

(4) Support and assist the 10 DISLAs, as identified in reference (n). Execute DON responsibilities identified in the Defense Infrastructure Sector Assurance Plan (DISAP), including coordination of DON risk management activities for DON owned critical assets and infrastructures that may also be identified as Sector critical assets and infrastructures.

e. In addition to other required reporting, within 24 hours of an event that degrades or destroys a DCA or Tier I TCA, notify the DON CIAO of the degradation or loss and the resulting impact on associated missions by the most expeditious method available. Within 96 hours of the initial report, submit a written plan of action and milestones to the DON CIAO, including actions taken or planned for remediation, recovery, or reconstitution. Submit monthly follow-up reports until resolved.

f. Coordinate all Service-level input for DoD and DON CIP policy through the DON CIAO. Advise the DON CIAO on policy recommendations for CIP issues.

g. Participate in the DON CIAO program review process and ensure the DON CIAO receives copies of DON DCA and Tier I TCA risk management products, e.g., assessment reports, risk management decisions.

h. Oversee the implementation of Service-level CIP policy. Ensure that all commanders, at every level, adhere to this policy and identify, validate, assess, and protect DCI within their command. Every installation and regional command, e.g., Navy and Marine Corps stations and bases, Navy and Marine Corps regional commands, and Marine Corps forces, with a DCA or TCA shall:

SECNAVINST 3501.1D
22 Jan 2018

(1) Appoint in writing a CIP point of contact to facilitate CIP coordination throughout the chain of command.

(2) Annually conduct and support CIP-related exercises to ensure mission and operational continuity, per references (h) and (i). CIP-related exercises may be incorporated into emergency preparedness actions or Service-directed assessment processes.

RISK MANAGEMENT

1. The DON CIP Program is a risk management program that seeks to ensure the availability of assets and infrastructure that are critical to planning, mobilizing, deploying, executing, and sustaining core DON capabilities, missions, and military operations. Risk management involves the application of a standardized process to identify, assess, and reduce risks and enable decision making that balances risk and cost with mission benefits. Applicable policy and detailed descriptions of the risk management process can be found in reference (i).

2. DON policy regarding CIP risk management includes:

a. Risk Assessment. Assessing risk is the foundation for executing an effective risk management program. Risk assessment involves a systematic, rational, and defensible process for identifying, quantifying, and prioritizing risks. Risk assessments shall include the collection and evaluation of data in three core areas: criticality assessment, all hazards threat assessment, and vulnerability assessment.

b. Risk Reduction Planning and Response

(1) Risk Management Decisions. The objective of the DON CIP Program is to manage risk to missions and assets, rather than managing vulnerabilities alone. The focus of risk management decisions shall be to achieve an acceptable level of risk in the execution of capabilities, missions, and military operations. The principal methods of managing risks include:

(a) Determining the likelihood of threat or hazard occurrence.

(b) Implementing risk remediation and mitigation countermeasures, e.g., physical security measures, personal protection measures, cybersecurity measures, emergency management planning, response and recovery, or asset redundancy.

(c) Acknowledging and reducing risk to an acceptable level. Decision makers may decide to acknowledge a particular risk when the impact of loss or the anticipated reduction in risk is not significant enough to justify the cost of the proposed risk countermeasure. At the recommendation of the DON

SECNAVINST 3501.1D
22 Jan 2018

CIP Program Working Group, the DON SE EXCOM may make risk acceptance determinations for DON critical assets, when the identified risk impacts the entire Department of the Navy and Marine Corps.

(2) Risk Response. Risk response includes making, documenting, implementing, and monitoring risk management decisions. Risk management decisions are documented using Risk Decision Packages representing one or more courses of action designed to address and reduce identified risk to asset and/or mission. The Navy and Marine Corps shall notify the DON CIAO of all risk management decisions for DCAs and Tier I TCAs.

ACRONYMS AND DEFINITIONS

Acronyms:

ASN (EI&E)	Assistant Secretary of the Navy for Energy, Installations, and Environment
ASN (FM&C)	Assistant Secretary of the Navy for Financial Management and Comptroller
ASN (M&RA)	Assistant Secretary of the Navy for Manpower and Reserve Affairs
ASN (RD&A)	Assistant Secretary of the Navy for Research, Development and Acquisition
AT	Antiterrorism
BEI	Baseline Elements of Information
BUMED	Bureau of Medicine and Surgery
CIAO	Critical Infrastructure Assurance Officer
CIP	Critical Infrastructure Protection
CCMD	Combatant Command
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
DCA	Defense Critical Asset
DCI	Defense Critical Infrastructure
DCIP	Defense Critical Infrastructure Program
DIB	Defense Industrial Base
DISAP	Defense Infrastructure Sector Assurance Plan
DISLA	Defense Infrastructure Sector Lead Agent
DoD	Department of Defense
DON	Department of the Navy
DUSN (P)	Deputy Under Secretary of the Navy for Policy
JP	Joint Publication
MEF	Mission Essential Function
MET	Mission Essential Task
NCIS	Naval Criminal Investigative Service
OASD (HD&GS)	Office of the Assistant Secretary of Defense for Homeland Defense and Global Security
OPR	Office of Primary Responsibility
SCM	Security Classification Manual
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SE EXCOM	Security Enterprise Executive Committee
TCA	Task Critical Asset
TS (SCI)	Top Secret (Sensitive Compartmented Information)
UNSECNAV	Under Secretary of the Navy
USG	United States Government

Definitions:

1. 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. (Source: reference (h))
2. Asset Owner. The DoD Components with responsibility for a DoD asset, or organizations that own or operate a non-DoD asset. (Source: reference (i))
3. Baseline Elements of Information (BEI). The minimum defined information requirements necessary to support a risk management decision. (Source: reference (i))
4. Benchmarks. For the purpose of this instruction, a series of necessary objectives-based questions for the DCIP, the answers to which indicate the degree to which specific standards have been met. (Source: reference (i))
5. Chemical, Biological, Radiological, and Nuclear Defense. An operational environment that includes chemical, biological, radiological, and nuclear threats and hazards and their potential resulting effects. (Source: Joint Publication (JP) 1-02 as amended through DoD Dictionary of Military and Associated Terms, August 2017) Also called CBRN defense. (JP) 3-11).
6. Continuity of Operations. An internal effort within individual DoD Components to ensure uninterrupted, essential DoD Component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and or attack-related emergencies. (Source: DoD Directive 3020.26 of 9 January 2009)
7. Critical Asset. Synonymous with TCA. See "Task Critical Asset" below.
8. Critical Asset Identification Process. A common analytical framework that is consistent and repeatable for use in identifying TCAs and DCAs through analysis and appropriate collaboration. (Source: reference (j))

9. Critical Infrastructure. Synonymous with DCI. See "Defense Critical Infrastructure" below.

10. Critical Infrastructure Assurance Officer (CIAO). The CIAO is responsible for the protection of all of the Department's critical infrastructures. The DON CIAO is DUSN (P), the chair of the DON SE EXCOM.

11. Critical Infrastructure Protection (CIP). Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. (Source: JP 1-02 as amended through 15 June 2014)

12. Critical Infrastructure Protection Program Working Group. The DON CIP Program Working Group is responsible for program policy implementation and execution feedback. The DON CIP Working Group is chaired by the DON CIP lead. Working Group membership is composed of the two Service CIP leads as well as action officers from the DON SE organizations representing the 10 DoD critical infrastructure sectors.

13. Criticality. For the purpose of this instruction, a metric used to describe the consequence of loss of an asset, based on the effect the incapacitation or destruction of the asset would have on DoD or DON operations and the ability of the DoD or DON to fulfill its missions. (Source: reference (i))

14. Cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (Source: DoD Instruction 8500.01 of 14 March 2014)

15. Defense Critical Asset (DCA). An asset of 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 DoD to fulfill its mission. (Source: reference (h))

16. Defense Critical Infrastructure (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 TCAs and DCAs. (Source: reference (h))

17. Defense Critical Infrastructure Program (DCIP). A DoD risk management program that seeks to ensure the availability of DCI. (Source: reference (h))

18. 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 DoD and are essential to the execution of the National Defense Strategy. (Source: reference (j)) The defense infrastructure sectors are:

a. Defense Industrial Base (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. (Source: reference (j))

b. Financial Services Sector. The DoD, USG, and private sector worldwide network and its supporting infrastructure that meet the financial services needs of the DoD across the range of military operations. (Source: reference (j))

c. DoD Information Network 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. (Source: reference (j))

d. Health 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. (Source: reference (j))

e. 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 reference (e). 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. (Source: reference (j))

f. 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. (Source: reference (j))

g. Personnel Sector. The DoD, USG, and private sector worldwide network that coordinates and supports personnel and human resource functions of DoD personnel. (Source: reference (j))

h. 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 DoD. (Source: reference (j))

i. 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 DoD. (Source: reference (j))

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

19. Defense Infrastructure Sector Assurance Plan (DISAP). Plan for a Defense Infrastructure Sector, developed and maintained by the appropriate DoD Component and DISLA, which includes 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 overall DCIP execution. The DISAP is updated yearly and provided to the OASD (HD&GS), appropriate DoD Components, and other DISLAs. (Source: reference (j))

20. Defense Infrastructure Sector Lead Agent (DISLA). Designated DoD officials and their respective defense organizations that perform defense infrastructure responsibilities. In coordination with their respective principal staff assistants, the DISLAs characterize their defense infrastructure sectors to identify functions, systems, interdependencies, and, ultimately, sector TCAs that support CCMD, Military Department, and Defense Agency missions and sector functions. (Source: reference (j))

21. Department of the Navy Security Enterprise Executive Committee (DON SE EXCOM). The senior-level governance body responsible for administration, strategic guidance, and policy authority for the DON SE. (Source: reference (p))

22. Force Protection. Preventive measures taken to mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information. (Source: JP 1-02 as amended through 15 June 2014)

23. Hazards. Non-hostile incidents, such as accidents, natural forces, and technological failure that cause loss or damage to infrastructure assets. (Source: reference (t))

24. 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 performance of DoD MEFs in any operating environment or condition. (Source: reference (o))

25. Mission Essential Functions (MEF). The specified or implied tasks required to be performed by, or derived from, statute, executive order, or other appropriate guidance, and those organizational activities that must be performed under all circumstances to achieve DoD Component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly affect DoD's ability to provide vital services, or exercise authority, direction, and control. (Source: DoD Directive 3020.26 of 9 January 2009)

26. Mission Essential Task (MET). A mission task selected by a commander deemed essential to mission accomplishment and defined using the common language of the universal joint task list in terms of task, condition, and standard. (Source: reference (j))

27. 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. (Source: reference (h))

28. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (Source: JP 1-02 as amended through 15 June 2014)

29. Reconstitution. The process by which surviving and/or replacement organization personnel resume normal organization operations from the original or replacement primary operating facility. (Source: Federal Continuity Directive 1 of October 2012)

30. Remediation. Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. (Source: reference (h))

31. Risk. Probability and severity of loss linked to threats or hazards and vulnerabilities. (Source: reference (h))

32. 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. (Source: reference (h))
33. Risk Management. A process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits. (Source: reference (h))
34. Risk Response. Actions taken to remediate or mitigate risk, or to reconstitute capability in the event of loss or degradation. (Source: reference (h))
35. Task Critical Asset (TCA). 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 Defense Infrastructure Section Lead Agent organizations to execute the task or MET it supports. TCAs are used to identify DCAs. (Source: reference (i))
36. Threat. An adversary having the intent, capability and opportunity to cause loss or damage. (Source: reference (h))
37. 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. (Source: reference (h))
38. Vulnerability Assessment. A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies, to identify vulnerabilities. (Source: reference (h))