



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 3501.1C
DON CIO
13 December 2011

SECNAV INSTRUCTION 3501.1C

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Ref: (a) DoD Directive 3020.40 of 14 January 2010
(b) DoD Instruction 3020.45 of 21 April 2008
(c) DoD 3020.45-M, Vol. 1, Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP), October 2008
(d) DoD 3020.45-M, Vol. 2, Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning, October 2008
(e) SECNAVINST 3030.4C
(f) DoD Instruction 2000.16 of 2 October 2006
(g) SECNAVINST 5000.2E
(h) DoD 3020.45-M, Vol. 3, Defense Critical Infrastructure Program (DCIP): Security Classification Manual (SCM), February 2011
(i) DoD 3020.45-M, Vol. 5, Defense Critical Infrastructure Program (DCIP): Execution Timeline, May 2010
(j) DoD Instruction 5240.19 of 27 August 2007

Encl: (1) Glossary
(2) Risk Management Process Model

1. Purpose. This instruction provides policy and delineates specific responsibilities for implementing critical infrastructure protection (CIP) in the Department of the Navy (DON). This instruction has been revised and should be reviewed in its entirety.

2. Cancellation. SECNAVINST 3501.1B.

3. Applicability and Scope. This directive applies to the Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), and the Commandant of the Marine Corps (CMC).

4. Definitions. Critical infrastructure terminology is defined in enclosure (1).

5. Background. References (a) through (j) provide policy and guidance for the protection of critical infrastructure within the Department of Defense (DoD) and the DON. The DON CIP Program plays an integral role in achieving mission assurance. Protection of the DON's critical infrastructure, both physical and cyber, requires proactive actions to identify potential vulnerabilities and make risk based determinations to remediate, and if degradation occurs, minimize the impact to overall mission. To that end, the DON critical infrastructure assurance officer (CIAO) has partnered with the Assistant Secretary of the Navy for Energy, Installations and Environment (ASN(EI&E)) to address the full spectrum of physical and cyber critical infrastructure. With this partnered approach, the DON CIP Program links numerous risk management program activities and security related functions (force protection (FP), computer network defense, and continuity of operations (COOP)) which support risk management decisions to enable continued execution of DON mission essential tasks (MET).

6. Policy. It is DON policy to:

a. Assure the availability of physical and cyber assets and infrastructure critical to planning, mobilizing, deploying, executing, and sustaining DON military operations on a global basis.

b. Support overall mission assurance by linking critical assets to DON and strategic missions in addition to coordinating and integrating activities with other DoD risk management programs.

c. Ensure the identification, prioritization, assessment, management of risk and protection of DON critical infrastructure are managed as a comprehensive program that includes the development of adaptive plans and procedures to mitigate risk,

restore capability, support incident management, and protect DON CIP related sensitive information (references (a), (b), (c), (d) and (e) are germane).

d. Use the results of the Risk Management Process Model, as detailed in enclosure (2), to determine needed funding and to obtain management approval of resources and actions for effecting changes in processes, practices or procedures to protect critical infrastructures or assets.

e. Remediate vulnerabilities in order to mitigate the risk of loss based on all threat and hazard risk management decisions made by responsible authorities.

f. Leverage and integrate CIP with other complementary mission assurance policies and programs focused on assuring, protecting and maintaining critical assets and infrastructure, particularly FP; COOP; chemical, biological, radiological, nuclear and high-yield explosives (CBRNE); and information assurance (IA) (references (e) and (f) are germane).

g. Support and assist the 10 defense infrastructure sector lead agents (DISLA), as identified in reference (a), in the:

(1) Identification, prioritization and protection of sector-related critical infrastructure.

(2) Execution of the defense infrastructure sector assurance plans (DISAP) and coordination of risk management activities with asset owners.

h. Support the defense critical infrastructure (DCI) sectors in the execution of their DISAP and coordination of risk management activities with asset owners.

i. Increase the awareness of the DON CIP Program by institutionalizing CIP policy within the Department and endorsing educational curricula, outreach, best practices and lessons learned.

j. Incorporate CIP policy as a critical element in acquisition, contracting and operations planning. Ensure requirements for the identification, prioritization, and protection of DCI are incorporated into requirements

development, acquisition planning, and acquisition, maintenance and sustainment contracts per references (a) and (g).

k. Periodically convene the DON CIP Program Council to oversee the governance, implementation and execution of the DON CIP policy.

l. Establish and periodically convene a DON CIP Program working group to coordinate DON CIP policy implementation among stakeholders.

m. Ensure written designation of points of contact (POC) for each DON defense critical asset (DCA) are provided to Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)) per reference (b).

n. Ensure that all DON critical asset data is maintained in an approved, ASD(HD&ASA) endorsed authoritative data base that can be accessed by DISLAs as well as both asset and mission owners.

o. Require, per reference (a), that Service CIP leads and other designated DON CIP Program personnel 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)). Classified material handling and safeguarding shall be done per reference (h).

7. Responsibilities

a. The Department of the Navy Chief Information Officer (DON CIO) shall serve as the DON CIAO and office of primary responsibility (OPR) for matters pertaining to critical infrastructure policy (both physical and cyber) in the DON (reference (a) germane) and shall:

(1) When the Secretary or Under Secretary is not available, represent the Secretary on DON CIP Program issues.

(2) Develop, publish, and maintain comprehensive policy and guidance for the DON CIP Program and oversee (including but not limited to) the implementation of:

(a) Major functional responsibilities and required program capabilities for both Navy Secretariat and Service CIP program leadership.

(b) An overarching DON CIP Program strategy which includes program vision and end state, program goals and objectives, and major program milestones.

(c) Critical asset identification across the Navy and Marine Corps using a mission focused process, per reference (c).

(d) Critical asset vulnerability assessments conducted per established DCIP standards and benchmarks.

(e) Asset risk determination using the Risk Management Process Model depicted in enclosure (2).

(f) Compilation, analysis, dissemination and sharing of program outputs, results and trends identified during assessments.

(g) Application of overarching guidance to ensure that CIP products and tools are interoperable throughout the DCIP community.

(3) Provide appropriate representation to the ASD (HD&ASA) and other Federal agencies for critical infrastructure issues. Specifically:

(a) Report on a semi-annual basis to the Office of ASD(HD&ASA) on organizational DCIP status and progress, consistent with references (a) and (b).

(b) When directed, provide to the Office of ASD(HD&ASA) a summary and review of the DON and Service CIP efforts and resource requirements.

(4) Oversee DON CIP Program initiatives and coordinate activities with the Secretariat, CNO and CMC as appropriate.

(5) Chair the DON CIP Program Council. Convene council meetings as needed, but at least annually, to determine resourcing and share findings, concerns, and best practices from

DON entities involved with or responsible for CIP mission assurance efforts. In addition, serve as the representative for the Global Information Grid defense sector.

(6) Serve as the overall manager and central POC for DON CIP Program related issues. This includes, but is not limited to, actions taken to establish and execute an organizational program supporting the DCIP.

(7) Collaborate with the DCIP community to establish and maintain an authoritative secure database of critical assets and associated data elements to:

(a) Provide for the secure storage of DON CIP related classified documents up to and including TS (SCI) per reference (a).

(b) Monitor remediation and other risk reduction efforts.

(8) Promote visibility and support for CIP related programmatic and budgetary expenditures; assist Service CIP leads in prioritizing resource requirements for the Programming, Planning and Budgeting System, per references (a) and (b).

(9) Maintain active liaison with other existing critical infrastructure related programs in the DoD, the Federal Government, and industry to:

(a) Share best practices.

(b) Seek economies in efforts required to assess and remediate organic and non-organic assets that are critical to DON warfighting readiness.

(10) As the chair, provide guidance as appropriate to the DON CIP Program Working Group.

(11) Develop information-sharing strategies for DON CIP Program initiatives, using existing tools and processes, to include:

(a) Establishing and issuing guidance as well as community best practices on key CIP program issues, including

risk management procedures and integrating COOP plans, ensuring consistency with existing DON, DoD, and Federal policy.

(b) Coordinating and facilitating data sharing relating to DON critical assets, assessment results, and the status of identified vulnerabilities and associated risk response actions.

(12) Ensure the development of new or modification of existing CIP program-related software tools, including self-assessment and risk management tools, can be utilized throughout the DON CIP community.

(13) Ensure DON critical assets and associated infrastructure dependencies, are identified by:

(a) Coordinating critical asset identification process actions, as detailed in reference (c), with ASN(EI&E), sector and service leads.

(b) Ensuring the DON critical asset list is properly updated to reflect changes in mission, technology, infrastructure, as well as DoD and DON requirements.

(c) At least annually, coordinating and reviewing all baseline elements of information (BEI) data.

(14) Coordinate and facilitate data sharing relating to DON critical assets, integrated vulnerability assessment (IVA) results, and remediation status of identified vulnerabilities.

(15) Coordinate with acquisition program and contract managers to ensure that requirements for the identification, prioritization, and protection of DCI are incorporated into acquisition, maintenance and sustainment contract development and follow references (a) and (g).

b. The ASN(EI&E) will assign a Deputy Assistant Secretary of the Navy to serve as the deputy CIAO; and in coordination with the DON CIAO, will have primary concentration on physical CIP with specific responsibilities that include:

(1) Oversee Service DCIP assessment programs and corresponding DON Core Vulnerability Assessment Management Program data as detailed in reference (f).

(2) Monitor service remediation and mitigation efforts to critical infrastructure.

(3) Oversee DON CIP and CIP related training and exercise implementation in the services.

(4) Coordinate with the DON CIAO and other DoD components and agencies to develop information sharing initiatives across the enterprise.

(5) Promote visibility and advocate for programmatic and budgetary expenditures.

(6) Develop guidance for the DON CIAO on key DON physical CIP issues, including remediation and mitigation, and ensuring consistency with existing DON, DoD and Federal policy as well as best practices.

(7) Coordinate all CIP related tasking through the DON CIAO.

(8) Participate as a member of the DON CIP Program Council.

(9) Provide senior subject matter experts knowledgeable in public works and environmental issues to the DON CIP Program Working Group and serve as the DON lead POC for the defense public works sector.

(10) Integrate critical infrastructure policy in the review of plans and policies, to include privatization, and public-private ventures; and make critical infrastructure policy an integral factor in directing ASN(EI&E) actions relating to facilities and utilities planning, design, construction, and maintenance.

c. The Assistant Secretary of the Navy, (Research, Development and Acquisition) shall:

(1) Serve as a member of the DON CIP Program Council.

(2) Serve as the DON primary POC and provide subject matter experts for the acquisition, defense industrial base (DIB), logistics, transportation and space defense sectors to the DON CIP Program Working Group.

(3) Work with the DON CIAO to identify, characterize, prioritize, and remediate vulnerabilities to critical non-organic infrastructures and processes managed by the acquisition community.

(4) Review policies that may be affected by critical infrastructure policy consideration and revise as necessary as directed by references (a) and (g). Require critical infrastructure 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 cycle of acquisition programs.

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

(1) Serve as a member of the DON CIP Program Council.

(2) Provide a senior financial sector subject matter expert to the DON CIP Working Group. Serve as the DON primary POC for the defense financial services sector.

(3) Be responsible for the oversight of DON critical financial infrastructures and develop risk management procedures for remediation, mitigation, and assurance that the minimum essential level of financial operations can be protected and maintained.

(4) Work with the other critical infrastructure sectors, as required, in addressing security requirements of DON financial infrastructures.

(5) Review policies that may be affected by critical infrastructure policy consideration and revise as necessary, making CIP an integral factor in policies directing ASN(FM&C) actions.

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

(1) Serve as a member of the DON CIP Program Council.

(2) Provide a senior DON personnel sector subject matter expert to the DON CIP Program Working Group. This individual shall serve as the DON lead POC for the defense personnel sector.

(3) Be responsible for the oversight of DON critical personnel infrastructures and develop risk management procedures for remediation, mitigation, and assurance that the minimum essential level of operations can be protected and maintained.

(4) Review policies that may be affected by critical infrastructure policy consideration and revise as necessary, making it an integral factor in policies directing ASN(M&RA) actions.

f. The CNO and CMC will assign an OPR within their respective Services with specific responsibilities that include:

(1) Prioritize, assess, manage risk and protect DON critical infrastructure.

(2) Identify, document and maintain a list of critical assets and associated supporting infrastructures per references (a) and (c).

(a) This list must be kept in a single DoD authoritative source accessible by the entire DCIP community. At a minimum, the critical asset list shall contain the BEI data for each critical asset as specified in reference (c) and comply with classification guidelines contained in reference (h).

(b) Provide for the secure storage of DON CIP related classified documents up to and including TS (SCI) per reference (a).

(3) Assess vulnerabilities, threats, hazards and determine risks to critical infrastructures and assets, per references (a), (b) and (f), implement risk response actions using appropriate DoD and DON guides, and monitor the results. Specifically:

(a) Coordinate with combatant commands (COCOMs), the Joint Staff, and defense infrastructure sectors, as needed, in identifying and scheduling critical infrastructures to be assessed by existing and future assessment processes.

(b) Establish a process to disseminate DCI related threat assessment and hazard warnings to installation commanders, CIP POCs, mission and asset owners.

(c) Remediate or reconstitute damaged or degraded critical assets, identify resource sponsors and asset owners responsible for DON critical infrastructures to understand the source(s) of funding available to affect a return to an operational state.

(d) Provide, maintain, and review critical infrastructure risk management data, and update accuracy and completeness of BEI data with all task critical asset (TCA) owners at least annually, per reference (j).

(e) Designate in writing a POC knowledgeable of each DCA; deliver a copy of the designation(s) to the DON CIAO for further delivery to the Office of ASD(HD&ASA) as per reference (b).

(f) Nominate critical assets for DCI risk assessment per references (a) and (j).

(4) In conjunction with the DON CIAO, establish an "all threats and hazards" risk management process, as set forth in paragraph 6 of this instruction and utilizing the Risk Management Process Model detailed in enclosure (2). This process is designed to:

(a) Have senior stakeholder decision makers acknowledge and accept the risk to associated critical infrastructures and assets; and

(b) Have DCIP standards and benchmarks, as issued by ASD(HD&ASA), incorporated into Service sponsored assessment processes.

(5) Provide senior subject matter experts familiar with service CIP issues to advise the DON CIP Program Council.

(6) Provide a CIP program lead representative to serve on the DON CIP Program Working Group.

(7) When tasked by the DON lead POC for the DCI sectors, identified in paragraph 7 of this instruction, organize senior subject matter experts to serve on service specific DON CIP sector working groups.

(8) Advise the DON CIAO on policy recommendations for critical infrastructure issues.

(9) Incorporate critical infrastructure policy into appropriate training and education programs.

(10) Work with the DON CIAO, the deputy CIAO, and the DON CIP Program Council to ensure the remediation of identified vulnerabilities and management of risk to critical infrastructures and assets are given appropriate consideration in the Planning, Programming, Budgeting, and Execution System.

(11) Initiate actions to ensure the availability and protection of critical assets and infrastructures, by:

(a) Integrating key activities, including other risk management programs and activities that address plans and procedures to remediate or mitigate risk, continue operations, restore capability in the event of loss or degradation, document risk decisions, support incident management and protect critical data.

(b) Regularly conducting DCIP related exercises focused on critical infrastructure to ensure mission and operational continuity per references (a) and (b). These DCIP related exercises may be incorporated into emergency preparedness actions or service directed assessment processes, e.g., CNO IVAs and U.S. Marine Corps mission assurance assessments.

(c) Providing DCIP information to the Office of ASD(HD&ASA), appropriate DoD components and DISLAs during: (1) defense support to civil authorities during emergency or first responder activity; or (2) consequence management operations and exercises.

(12) Ensure, at a minimum, every installation and regional command, e.g., Navy and Marine Corps stations and bases, Navy regional commands and Marine Corps forces, appoint in writing a CIP POC to facilitate CIP coordination throughout the chain of command.

(13) Establish the necessary and appropriate lines of communication and promote information sharing with other Federal, State, and local entities. Ensure both the DON CIAO and deputy CIAO are advised of all CIP program coordination efforts, including contact with COCOMs, DoD and DON infrastructure sector managers.

(14) In addition to any other required reporting, within 48 hours of a disruptive event, or the discovery of a significant vulnerability surfaced during the course of an assessment, apprise the DON CIAO of any degradation, damage, or loss of tier 1 DON critical asset(s) and the resulting impact on the associated MET by the most expeditious method available. Within 96 hours of the initial report, submit a plan of action and milestones in writing to the DON CIAO, which will include actions taken or planned for remediation, recovery or reconstitution. Submit monthly follow-up reports until resolved.

(15) Review policies that may be affected by critical infrastructure policy consideration and revise as necessary, making CIP an integral factor in policies directing actions and programs. Incorporate requirements for the risk management of DCI in acquisition, maintenance, and sustainment contract development, as well as in facility construction, installation recapitalization, and installation-level outsourcing and privatization efforts.

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

(1) Serve as a member of the DON CIP Program Council.

(2) Provide a representative to the DON CIP Program Working Group, knowledgeable in the areas of vulnerability assessments and indications and warning (I&W). Serve as the DON primary POC for the defense intelligence, surveillance, and reconnaissance sector.

(3) In partnership with the Office of Naval Intelligence and the Office of the Under Secretary of the Navy, Assistant for Special Programs/Intelligence, coordinate with the DON CIAO in developing a comprehensive I&W capability for threats to critical infrastructures and assets from unconventional sources, i.e., foreign intelligence services, terrorism, etc.

(4) Provide DCIP focused counterintelligence protection to the DON and the defense sector lead organizations per references (a), (b) and (i). This coverage will include, but not be limited to, providing threat and vulnerability assessments for DCI where the asset owner is the DON or a DoD affiliated organization tasked to NCIS. This support shall include the dissemination of this information to DON installation commanders, and Department and Service CIP POCs.

(5) In coordination with the DON CIAO, prepare and provide intelligence production requirements annually in order to carry out CIP responsibilities on Navy or Marine Corps owned DCI to be monitored for threats per reference (a).

(6) In coordination with the Services, provide DCIP assessment capability which incorporates DCIP standards and benchmarks, as issued by ASD(HD&ASA).

(7) Assist Service CIP POCs in the identification of critical infrastructure and asset vulnerabilities and the development of remediation strategies.

(8) Review policies that may be affected by critical infrastructure policy consideration and revise as necessary, making it an integral factor in policies directing NCIS actions and programs.

h. The Surgeon General/Chief Bureau of Medicine and Surgery shall:

(1) Serve as a member of the DON CIP Program Council.

(2) Provide a representative to the DON CIP Program Working Group, knowledgeable in the area of health related threats and vulnerabilities. Serve as the DON lead POC for the defense health affairs sector.

(3) Review policies that may be affected by CIP policy consideration and revise as necessary, making it an integral factor in policies directing actions and programs.

i. The DON CIP Program Council is responsible for providing senior level leadership, program oversight and guidance. Council membership is composed of representatives mirroring the 10 DoD critical infrastructure sectors as described in reference (a). The council shall:

(1) Determine the necessary efforts to institutionalize DON critical infrastructure policy implementation to ensure warfighter mission assurance.

(2) Monitor progress of DON CIP Program implementation and activities, making policy change recommendations, and directing appropriate actions to support the Navy and Marine Corps team effort in ensuring the mission assurance for the COCOMs in the execution of the National Military Strategy.

(3) Seek to foster CIP program cooperation and collaboration within the DON, DoD and other Federal organizations to improve program effectiveness.

(4) Contribute subject matter expertise to support the DISLA.

(5) Recommend resource actions to support DON CIP Program implementation, risk management, remediation and continued mission assurance through protection of DON critical assets and associated infrastructures.

j. The DON CIP Program Working Group is responsible for program policy implementation and execution feedback. Working group membership is composed of the two CIP program service leads, as well as action officers from the U.S. Navy and U.S. Marine Corps appointed by the DON CIP Program Council member organizations representing the 10 DoD critical infrastructure sectors as described in reference (a), and shall:

(1) Be comprised of senior subject matter experts at the O-5/O-6 or civilian equivalent grade.

(2) Meet as needed in support of continuing DON CIP Program initiatives; report progress to, and receive direction from, the DON CIP Program Council.

(3) Institutionalize the DON CIP Program implementation throughout the DON to ensure warfighter mission assurance.

(4) Facilitate cooperation and collaboration within the Department and in policy matters with DoD and other Federal organizations to improve DON CIP Program effectiveness.

(5) Recommend resource actions to support DON CIP Program implementation, risk management, remediation and continued mission assurance through protection of DON critical assets and associated infrastructures.

(6) Provide input to support future policy.

8. Procedures. The DON CIP Program supports a risk management process, as detailed in enclosure (2), which seeks to ensure critical asset availability. For the DON CIP Program, this risk management process:

a. Identifies critical assets and infrastructure interdependencies supporting DoD missions;

b. Includes a risk assessment comprised of mission focused, all hazards, threats, and vulnerability assessments; and

c. Enables informed risk management decisions by asset and mission owners, leading to an appropriate risk response so that limited resources are optimally allocated toward those assets deemed most important to overall mission success.

9. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of November 2007.

SECNAVINST 3501.1C
13 December 2011

10. Reports Control. The reporting requirements contained in this instruction are exempt from licensing following part IV, paragraph 7, subparagraph 1, of SECNAV Manual 5214.1 of December 2005.



TERRY A. HALVORSEN
Department of the Navy Chief
Information Officer

Distribution:

Electronic only, via Department of the Navy Issuances Web site
<http://doni.daps.dla.mil>

GLOSSARY

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 owned or operated by domestic foreign, public or private sector organizations. (Source: reference (a))
2. Consequence Management. Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. (Source: CJCSI 3112.01A)
3. Continuity of Operations (COOP). 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)
4. Critical Asset. Synonymous with TCA. See "Task Critical Asset" below.
5. Critical Asset List. A compilation of infrastructure TCAs determined to be essential to the execution of directed mission responsibilities.
6. Critical Infrastructure. Synonymous with DCI. See "Defense Critical Infrastructure" below.
7. Critical Infrastructure Assurance Officer (CIAO). The CIAO is responsible for the protection of all of the Department's critical infrastructures. The DON CIAO is the DON CIO and chairs the DON CIP Program Council.
8. 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. (Source: JP 1-02)

9. Critical Infrastructure Protection Program Council. The DON council comprised of senior civilian leadership, flag and general officers who support the DON CIAO in decision-making and leadership for CIP in the DON. The DON CIP Program Council will convene periodically to oversee the governance, implementation and execution of CIP within the Department.

10. 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 CIAO and co-chaired by the deputy CIAO. Working group membership is composed of the two CIP service leads as well as action officers from the DON CIP Program Council member organizations representing the 10 DoD critical infrastructure sectors.

11. Cyber Infrastructure. Includes electronic information and communication systems, and the information contained in these systems. Computer systems, control systems such as Supervisory Control and Data Acquisition systems, and networks such as the Internet are all part of cyber infrastructure. (Source: National Infrastructure Protection Plan, 2009)

12. Defense Critical Asset. 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 (a))

13. 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 defense critical assets. (Source: reference (a))

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

15. 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 (a))

16. Hazard. Non-hostile incidents, such as accidents, natural forces, technological failure, that cause loss or damage to infrastructure assets. (Source: reference (a))

17. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporation protection, detection, and reaction capabilities. (Source: DoD Directive 8500.01E of 24 October 2002)

18. Information Systems. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (Source: CNSS Instruction No. 4009 of 26 April 2010)

19. 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. (Source: reference (a))

20. Mission Assurance. A process to ensure that assigned tasks or duties can be performed following 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 FP; antiterrorism; CIP; IA; COOP; CBRNE defense; readiness; and

installation preparedness-to create the synergistic affect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. (Source: reference (a))

21. Mission Essential Function (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)

22. 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 (c))

23. 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 (a))

24. 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)

25. Reconstitution. The process by which surviving and or replacement agency personnel resume normal agency operations from the original or replacement primary operating facility. Reconstitution embodies the ability of an agency to recover from an event that disrupts normal operations and consolidates the necessary resources so that the agency can resume its operations as a fully functional entity of the Federal Government. In some cases, extensive coordination may be necessary to procure a new operating facility, if an agency suffers the complete loss of a

facility or in the event that collateral damage from a disaster renders a facility structure unsafe for reoccupation. (Source: Federal Continuity Directive 1 of February 2008)

26. Remediation. Actions taken to correct known deficiencies and weaknesses. These actions are undertaken once vulnerability has been identified. (Source: reference (a))

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

28. 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 (a))

29. 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 (a))

30. Risk Response. Actions taken to remediate or mitigate risk, or to reconstitute capability in the event of loss or degradation. (Source: reference (a))

31. 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 DISLA organizations to execute the task or MET it supports. TCAs are used to identify defense critical assets. (Source: reference (a))

32. Threat. An adversary having the intent, capability and opportunity to cause loss or damage. (Source: reference (a))

33. 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 (a))

SECNAVINST 3501.1C
13 December 2011

34. Vulnerability Assessment. A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies, to identify vulnerabilities. (Source: reference (a))

RISK MANAGEMENT PROCESS MODEL

1. The heart of the DON CIP Program is a risk management process that seeks to ensure critical asset availability. Risk assessment and risk response are the major elements of risk management. The component parts of risk assessment and risk response and their relationship to one another are illustrated below in figure (1).

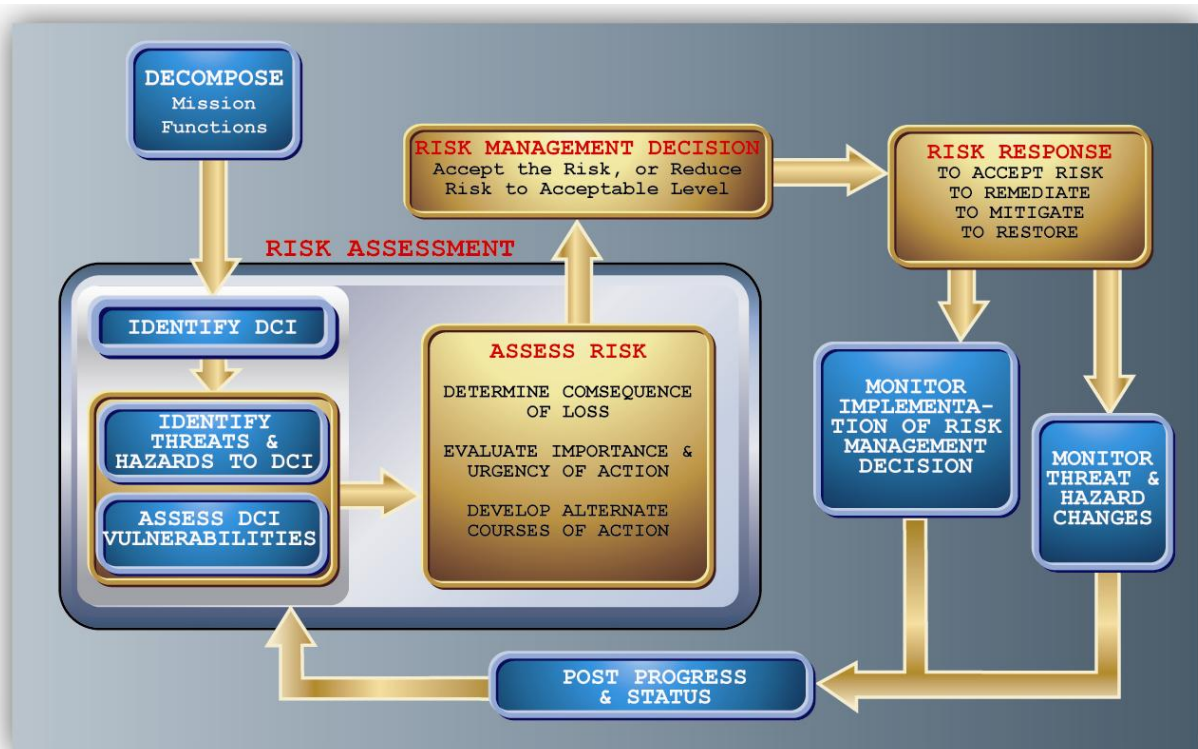


Figure 1. Risk Management Process Model

a. The core elements of the Risk Management Process Model are criticality determination, threats and hazards assessment, and vulnerability assessment. For complete and accurate risk assessment, the evaluation of each element must be accomplished individually and collectively, as well as the assessment of the interactions and interdependencies involved (criticality, threat and or hazard, vulnerability).

b. A detailed description of each of the elements comprising the Risk Management Process Model can be found in reference (b).

2. Risk elements span activities that occur before, during, and after natural or man-made events, which may result in infrastructure compromise or disruption. A key aspect of the DON CIP Program recognizes the relationships and the importance of DON assets and installations with critical infrastructures that support both title 10 and COCOM requirements, particularly operations plans. DON policy is to:

a. Identify and prioritize METs, core functions and associated critical assets; assess and protect physical and cyber infrastructures deemed critical to DON force and materiel readiness and operations in peace, crisis, and war; mitigate the effect of their loss or disruption; and plan for timely restoration or recovery.

b. Coordinate or consult, as appropriate, with the necessary Federal, State and local agencies to implement a standardized process for DCI and inter- and intra-dependency identification.

c. Effectively manage risk through a centralized process to ensure critical DON equipment and facilities, utilities, services, and weapon systems supporting mission accomplishment are monitored and protected and all hazards and threat data are considered. Critical assets can be highly dependent upon supporting non-organic assets, including national or international infrastructures, facilities and services of the private sector, DIB, and other government departments and agencies.

d. Observe, report, and manage risk determination action(s) required for the protection, remediation or mitigation of non-organic infrastructures and assets whose security responsibility is primarily with the private and non-government asset owners and with local, State, and Federal law enforcement authorities; including non-United States infrastructures and assets that are the responsibility of appropriate foreign and national authorities for protection.