



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

SECNAVINST 3501.1B
DON CIO
5 February 2010

SECNAV INSTRUCTION 3501.1B

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Ref: (a) DoD Directive 3020.40 of 19 Aug 05
(b) DON Consequence Management (CM) Planning Guide, Second Edition, 2004
(c) DoD Instruction 3020.45 of 21 Apr 08
(d) DoD Manual 3020.45, Vol. 1, of 24 Oct 08
(e) SECNAVINST 5000.2D
(f) UNSECNAV memo of 26 Aug 99, DON Critical Infrastructure Protection (NOTAL)
(g) Homeland Security Presidential Directive/HSPD-7 of 17 Dec 03
(h) DoD Manual 3020.45, Vol. 2, of 28 Oct 08
(i) SECNAVINST 3030.4C
(j) DoD Instruction 2000.16 of 2 Oct 06

Encl: (1) Glossary
(2) Risk Management Process Model
(3) DON Critical Infrastructure Protection Program Quarterly Status Report Format

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 3501.1A.

3. Applicability and Scope. This directive applies to the Offices of the Secretary of the Navy, 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 (h) provide policy and guidance for the protection of critical infrastructure within the Department of Defense (DoD) and the Department of the Navy. The DON CIP Program plays an integral role in achieving mission assurance (MA). Protection of the DON's critical infrastructure, both physical and cyber, requires participation by all hands to identify potential vulnerabilities, defend against exploitation, and if exploited, 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 Installations and Environment (ASN (I&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). The DON CIP Program supports overall MA by linking critical assets, both physical and cyber, to DON missions.

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. 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 (i) germane).

c. 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.

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

e. Leverage and integrate CIP with other complementary MA 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 (i) and (j) are germane).

f. Support and assist the 10 Defense infrastructure sector lead agents (DISLA) to identify, prioritize and protect sector-related critical infrastructure. As detailed in reference (a), the Defense critical infrastructure sectors are:

- (1) Defense Industrial Base (DIB).
- (2) Financial Services.
- (3) Global Information Grid (GIG).
- (4) Health Affairs.
- (5) Intelligence, Surveillance, and Reconnaissance (ISR).
- (6) Logistics.
- (7) Personnel.
- (8) Public Works.
- (9) Space.
- (10) Transportation.

g. Support the Defense critical infrastructure sectors in the execution of their Defense infrastructure sector assurance plans and coordination of risk management activities with asset owners.

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

i. Incorporate CIP policy as a critical element in acquisition, contracting and operations planning in accordance with reference (e). Acquisition program and contract managers shall ensure requirements for the identification, prioritization, and protection of defense critical infrastructure are incorporated into acquisition, maintenance and sustainment contracts and are in accordance with references (a) and (e).

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

k. Establish and periodically convene a DON CIP Program Working Group to coordinate DON CIP policy implementation among stakeholders.

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 Department of the Navy (references (a) and (f) germane) and shall:

(1) Represent the Secretary (when the Secretary or Under Secretary are not available) on DON CIP Program issues.

(2) Provide policy and guidance for the DON CIP Program and oversee (including but not limited to) the implementation of:

(a) Service CIP program responsibilities.

(b) An overarching DON CIP Program strategy.

(c) Critical asset identification across the Navy and Marine Corps using a mission focused process, in accordance with references (c) and (d).

(d) Critical asset vulnerability assessments conducted in accordance with established Defense Critical Infrastructure Program (DCIP) standards and benchmarks.

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

(f) Compilation and analysis of trends identified during vulnerability 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 Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD (HD&ASA)) and other Federal Agencies for critical infrastructure issues.

(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, share findings, concerns, and best practices from DON entities involved with or responsible for CIP MA efforts. In addition, serve as the representative for the GIG Defense Sector.

(6) Serve as the overall manager and central point of contact 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; collaborating with entities; establishing and maintaining a secure database of DON critical assets and associated data elements; monitoring remediation efforts; promoting visibility and support for programmatic and budgetary expenditures; and maintaining active liaison with other existing critical infrastructure related programs in the Department of Defense, the Federal Government, and industry in order to:

(a) Establish and promulgate DON CIP Program policy.

(b) Share best practices.

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

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

(8) Develop information-sharing strategies for DON CIP Program initiatives, using existing tools and processes. Promulgate guidance for DON entities on key CIP program issues, including risk management procedures and integrating COOP plans, ensuring consistency with existing DON, DoD, and Federal policy as well as community best practices.

(9) 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.

(10) Ensure DON critical assets and associated infrastructure dependencies, are identified.

(a) Coordinate critical asset identification process actions, as detailed in reference (d), with ASN (I&E), sector and service leads.

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

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

(a) Ensure that all task critical asset (TCA) owners (commanding officers or officer-in-charge, as applicable) review and update baseline elements of information (BEI) data for their assets at least annually.

(b) Review and update BEI data with all DON defense critical asset owners at least annually.

b. The ASN (I&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) Oversight of the vulnerability assessment program and corresponding DON Core Vulnerability Assessment Management Program data as detailed in reference (j).

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

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

(4) Coordinating 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 point of contact 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 (I&E) actions relating to facilities and utilities planning, design, construction, and maintenance.

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

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

(2) Serve as the DON primary point of contact and provide subject matter experts for the acquisition, 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, making it an integral factor in policies directing ASN (RD&A) actions.

(5) Require critical infrastructure policy consideration in acquisition management procedures by incorporating requirements for the identification, prioritization, and protection of Defense critical infrastructure in the life cycle of acquisition programs, as directed by references (a) and (e).

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 point of contact 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 it 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 point of contact 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 Director, Naval Criminal Investigative Service (NAVCRIMINVSERV) 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 point of contact for the Defense ISR 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 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) Incorporate established DCIP standards and benchmarks, as promulgated by ASD (HD&ASA), into vulnerability assessments.

(5) Assist in the identification of critical infrastructure and asset vulnerabilities and the development of remediation strategies.

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

g. 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 point of contact 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.

h. The CNO and CMC shall:

(1) Identify an OPR for matters pertaining to the identification, prioritization, assessment, management of risk and protection of DON critical infrastructure. Establish, resource and execute an organization program supporting this policy.

(2) Identify and document critical assets and associated supporting infrastructures in accordance with references (c) and (d).

(a) In order to 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 effect a return to an operational state.

(b) Review and update BEI data with all TCA owners at least annually, but no later than 30 April.

(3) Assess vulnerabilities to critical infrastructures and assets, per references (a) and (j), using appropriate DoD/DON guides. (See references (b) and (d)). Coordinate with combatant commanders (COCOMs), the Joint Staff, and Defense infrastructure sectors as needed in identifying and scheduling critical infrastructures to be assessed by existing and future IVA processes.

(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), to determine the acceptable risk to associated critical infrastructures and assets. Incorporate established DCIP standards and benchmarks, as promulgated by ASD (HD&ASA), into CNO IVAs.

(5) Not later than the 15th of February, May, August and November, report in writing to the DON CIAO the status of CIP program efforts for the preceding quarter to include: assessments planned or completed; vulnerabilities identified; remediation actions initiated; resource issues and other data elements using the reporting format provided in enclosure (3).

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

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

(8) When tasked by DON lead point of contact for the Defense critical infrastructure sectors, identified in paragraphs 6 and 7 of this instruction, organize senior subject matter experts to serve on service specific DON CIP sector working groups.

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

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

(11) 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.

(12) Initiate actions to ensure the availability and protection of critical assets and infrastructures to include the integration of key 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.

(13) 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, appoints in writing a CIP point of contact to facilitate CIP coordination throughout the chain of command.

(14) Ensure both the DON CIAO and Deputy CIAO are advised of CIP program coordination efforts with COCOMs, DoD and DON infrastructure sector managers.

(15) 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 DON critical asset(s) (tiers I, II, and III) 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.

(16) 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.

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 MA.

(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 MA for the COCOMs in the execution of the National Military Strategy.

(3) Seek to foster CIP program cooperation and collaboration within the Department of the Navy, Department of Defense 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 MA 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 0-5/6 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 Department of the Navy to ensure warfighter MA.

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

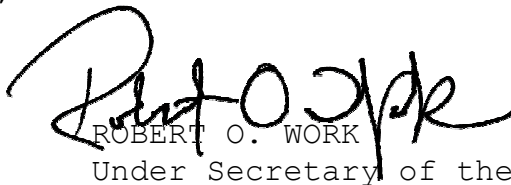
(5) Recommend resource actions to support DON CIP Program implementation, risk management, remediation and continued MA through protection of DON critical assets and associated infrastructures.

(6) Provide input to support future policy.

8. Procedures. The DON CIP Program supports a risk management process that seeks to ensure critical asset availability. For the DON CIP Program, this risk management process is comprised of an assessment component that identifies critical assets and infrastructure interdependencies supporting DoD missions. Applicable follow-on threat and vulnerability assessments are then conducted on those assets to complete the risk assessment. Properly implemented risk assessment procedures of critical assets enable informed risk management decisions by mission owners, leading to an appropriate risk response. The risk response component ensures that limited resources are optimally allocated toward those assets deemed most important to overall mission success, and for which it has been determined that the identified level of risk is unacceptable. Detailed program procedures are outlined in enclosure (2).

9. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed in accordance with SECNAV Manual 5210.1.

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


ROBERT O. WORK
Under Secretary of the Navy

Distribution:

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

Glossary

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. (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. How a command manages the consequences of an event directly impacts its ability to maintain COOPs. (Source: reference (b))
3. Continuity of Operations (COOP). An internal effort within individual components of the Executive, Legislative, and Judicial Branches of Government assuring the capability exists to continue uninterrupted essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack-related emergencies. COOP involves plans and capabilities covering the same functional objectives of continuity of government (COG), must be maintained at a high level of readiness, and be capable of implementation both with and without warning. COOP is not only an integral part of COG and enduring constitutional government, but is simply "good business practice" - part of the DoD's fundamental mission as a responsible and reliable public institution. (Source: DoD Directive 3020.26 of 9 Jan 09)
4. Critical Asset. Sometimes referred to as a task asset; an asset that is directly used to support execution of one or more operations, tasks, activities, or METs. (Source: reference (c))
5. Critical Asset List. A compilation of infrastructure items determined to be essential to the execution of directed mission responsibilities.
6. Critical Infrastructure. DoD and non-DoD networked assets essential to project support and sustain military forces and operations worldwide. (Source: reference (a))

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. (Source: reference (f))

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: reference (a))

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 Department of the Navy. 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. That portion of the critical infrastructure that includes electronic information and communications systems and services and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of these elements. (Source: National Infrastructure Protection Plan, 2006)

12. Defense Critical Asset. An asset of 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 mission. (Source: reference (a))

13. Defense Critical Infrastructure. DoD and non-DoD networked assets essential to project support and sustain military forces and operations worldwide. (Source: reference (a))

14. 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. (Source: reference (a))

15. Defense Industrial Base (DIB) Sector. The commercial, private sector worldwide industrial complex with capabilities to perform research and development, design, produce and maintain military weaponry systems, subsystems, components or parts to meet military requirements. (Source: reference (a))

16. Hazard (Infrastructure). 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 Oct 02)

18. 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. (Source: reference (a))

19. 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 ISR information, in support of activities that meet the needs of DoD users across the range of military operations. (Source: reference (a))

20. Mission Assurance (MA). 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 Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security related functions-such as FP; antiterrorism; CIP; IA; COOPs; CBRNE defense; readiness; and installation preparedness-to create the synergistic affect required for Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. (Source: reference (a))

21. Mission Essential Task (MET). Specified or implied tasks required to be performed by, or derived from, statute or Executive order, 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 impact DoD ability to provide vital services, or exercise authority, direction, and control. (Source: DoD Directive 3020.26 of 9 Jan 09)

22. 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))

23. Monitoring and Reporting. The collection, fusion and dissemination of intelligence-based I&Ws, 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. (Source: reference (a))

24. Network. A group or system of interconnected or cooperating entities, normally characterized as being nodes (assets), and the connections that link them. (Source: reference (a))

25. 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: Joint Publication JP 1-02)

26. 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 Feb 08)

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

28. Response. Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include: applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice. (Source: National Response Plan - Homeland Security Dec 04)

29. Risk. Probability and severity of loss linked to threats or hazards. (Source: reference (a)) The possibility that a particular threat will adversely impact an asset by exploiting a particular vulnerability. (Clarification added by DON CIO)

30. Risk Management. A process by which decision makers accept, reduce, or offset risk. (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 DISLAs to execute the task or MET it supports. TCAs are used to identify defense critical assets. (Source: reference (c))

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

33. 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. (Source: reference (a)) A weakness that could be exploited. (Clarification added by DON CIO)

34. Vulnerability Assessment (Infrastructure). 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).

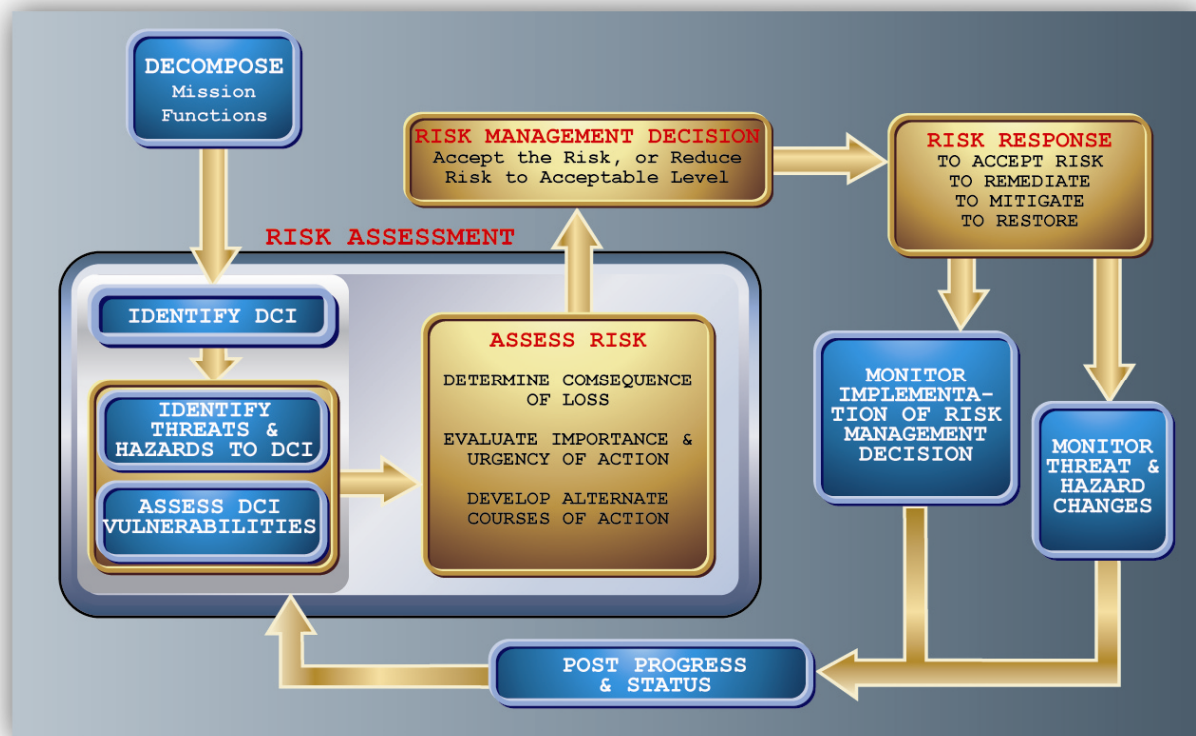


Figure 1. Risk Management Process Model

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, collectively, and in consonance 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 (c).

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 X 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. 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 hazard" threat data is 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.

c. 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.

DON Critical Infrastructure Protection Program
Quarterly Status Report Format

Classify in accordance
With CIP Security
Classification Guide

Date

From: OPNAV (N4) or HQMC (PPO)
To: DON CIAO

Subj: DON CRITICAL INFRASTRUCTURE PROTECTION PROGRAM QUARTERLY
STATUS REPORT FOR THE MONTHS OF xxxx, xxxx, and xxxx 20xx

1. List the Defense Critical Infrastructure Program (DCIP) assessments (e.g., Joint Service Integrated Vulnerability Assessment (JSIVA); CNO Integrated Vulnerability Assessment (IVA), etc.), completed during the past quarter.

<u>Location</u>	<u>Date</u>	<u>Type</u>
a.		
b.		
c.		

2. Highlight the significant findings and areas of concern identified by the assessments completed during the past quarter. Categorize these findings by benchmark area, i.e., Antiterrorism/Force Protection, Emergency Management/COOP, DCIP Electric Power, Cyber, etc., and evaluate their potential mission essential task impact.

<u>Benchmark Area</u>	<u>Impact (H/M/L)</u>	<u>MET</u>
a.		
b.		
c.		

3. Summarize the planned remediation actions for the items listed in paragraph 2. Categorize all planned measures in one

or more of the following remediation action categories:
doctrine changes, organization changes, training, material,
governance, personnel changes, or facilities.

4. Summarize resources required to effect the remediation actions listed above, along with the responsible resource sponsor. Note status of required resources, i.e., whether or not included in Program Objective Memorandum/Program Review or budget; if not explain what steps are being taken to address resource shortfall.

5. List the DCIP assessments (e.g., JSIVA; CNO IVA, etc.), planned for the upcoming 3-month period.

<u>Location</u>	<u>Date</u>	<u>Type</u>
a.		
b.		
c.		

(*) Due NOT LATER THAN the 15th of
February, May, August and November annually.

Copy to:
Deputy CIAO (ASN (I&E))