



DEPARTMENT OF THE NAVY

CRITICAL  
INFRASTRUCTURE  
PROTECTION PROGRAM  
STRATEGY FOR 2009 AND BEYOND

STRATEGY  
MAY 2009



## Foreword

Presidential Decision Directive/NSC-63 (PDD-63), Critical Infrastructure Protection was released in 1998 in recognition of the need for a national effort to assure the security of our nation's increasingly vulnerable and interconnected infrastructure. It was followed by Homeland Security Presidential Directive/HSPD-7, which established a national policy for Federal departments and agencies to identify, prioritize and protect United States critical infrastructures and key resources.

We have made great progress in the Department of the Navy (DON) through our teaming efforts with the Assistant Secretary of Defense (Homeland Defense & America's Security Affairs), the Defense Threat Reduction Agency, our participation in the Chief of Naval Operations - Integrated Vulnerability Assessment process, and the publication of the DON Consequence Management and Remediation Planning Guides. However, the threat to our infrastructure and information is advanced, persistent, sophisticated, always changing, and well resourced. Our challenge is to be more advanced, more persistent, more sophisticated, and stay ahead of the threat to ensure we are able to meet mission requirements. We can do so by smartly and effectively focusing our increasingly limited resources and working together as a community with Government and industry to develop solutions.

This strategy outlines our path forward for the Critical Infrastructure Protection Program within the DON.

Robert Carey  
Department of the Navy Chief Information Officer

Department of the Navy

# Critical Infrastructure Protection Program

Strategy for 2009 and Beyond

## Strategy Purpose

The Department of the Navy (DON) relies on a network of physical and cyber infrastructure so critical that its degradation, exploitation, or destruction could have a debilitating effect on the DON's ability to project, support, and sustain its forces and operations worldwide. This critical infrastructure includes DON and non-DON domestic and foreign infrastructures essential to planning, mobilizing, deploying, executing, and sustaining U.S. military operations on a global basis. Mission Assurance is a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is made more difficult due to increased interconnectivity and interdependency of systems and networks. DON critical infrastructures, both physical and cyber, even if degraded, must be available to meet the requirements of multiple, dynamic, and divergent missions.

Protecting DON critical assets and ensuring the availability of its mission essential functions is the key tenet of the DON Critical Infrastructure Protection (CIP) Program. The demand for resources to protect DON critical infrastructure far exceeds available resources and the foreseeable future reflects little change in that posture. However, the limited availability of resources in no way diminishes the need to ensure that infrastructure assets critical to the execution of Navy and Marine Corps missions are available. The DON will employ a risk management process to guide investment and resourcing decisions in order to meet mission execution requirements – both tactical as well as strategic.



Figure 1: Mission Assurance Risk Management Process Model

### Risk Management Process

The naval services must be able to share information with each other and with DoD, and leverage the collective body of work available not only within the DON, but across the entire Defense Critical Infrastructure Program community. Most importantly, in recognition of the fact that not all of the Department’s assets can be protected, the DON must implement and follow through with an operationally focused CIP Program Risk Management Process Model as depicted in Figure 1.

This approach starts with a focus on mission and the identification of those infrastructures or assets, physical and cyber, that are critical to planning, mobilizing, deploying, executing, and sustaining military operations globally, using the Critical Asset Identification Process (CAIP). The CAIP, which is a mission-focused process for the identification of Defense Critical Infrastructure (DCI), is a critical first step in this model. Vulnerability and threat assessments, which are central to this process, help to determine which assets are most at risk and the impact of potential loss on the mission. The overall risk assessment is based on consideration of the criticality of the asset/infrastructure, threats and vulnerabilities, and the probability of a disruptive event occurring. After assessing the risk, a coordinated and informed risk management decision can then be made on which courses of action to take, utilizing a sound defense-in-depth solution that includes people, processes, and technology, with no break in the cycle. This

model, along with the CAIP, is further defined in a forthcoming update to the Department of the Navy Critical Infrastructure Protection Program instruction.

Historically, the approach to critical infrastructure protection within the DON has focused heavily on physical infrastructure, and largely aligned with antiterrorism efforts. However, as critical infrastructures increasingly rely on computers and networks for their operations, the DON Critical Infrastructure Protection Program must expand its focus to encompass physical as well as cyber infrastructures, as defined in Figure 2. This expanded focus will also require different approaches to remediate cyber infrastructure vulnerabilities.



Figure 2: Risk Decision Process Model

### Objectives for the Future

- Identify and document critical assets and infrastructures;
- Assess vulnerabilities to critical assets and infrastructures;
- Establish a risk management process to determine the maximum level of acceptable risk to identified critical assets and infrastructures, based on their contribution to warfighting mission and system vulnerability;
- Ensure the remediation of identified vulnerabilities to critical assets and infrastructures are given appropriate consideration in the planning, programming, budgeting, and execution system (PPBES); and

- Incorporate Critical Infrastructure Protection Program principles into appropriate training programs.

To ensure we are able to accomplish the objectives for 2009 and the challenges of the future, we must work together. Within the DON, we have developed a CIP Self Assessment Tool (CIP SAT), which is now undergoing the certification and accreditation process. CIP SAT will be available to assess those critical assets identified through the CAIP process. We applaud the efforts of the Marine Corps in the development and implementation of the Marine Corps Critical Asset Management System (MCCAMS), and their willingness to share with the Navy. We must move forward in the ability to maintain and share DON CIP data with appropriate Joint Staff and Combatant Command (COCOM) entities through the use of the Strategic Mission Assurance Data System (SMADS) and our DON interoperable information management systems.

## The Path Forward

The DON CIP Program has numerous challenges for the future and we must work together to find mutual solutions. The DON Critical Infrastructure Protection Program will foster mission assurance by establishing policy and oversight to:

1. Align with the Department of Defense (DoD) Assistant Secretary of Defense (Homeland Defense and America's Security Affairs (ASD(HD&ASA))).
  - a. Comply with the policy provided in DOD Directive 3020.40, DOD Instruction 3020.45, and other published policy;
  - b. Participate in the Defense Critical Infrastructure Integration Staff (DCIIS), the Operational Advisory Board (OAB), and other coordination meetings;
  - c. Maintain and share DON CIP data with appropriate Joint Staff, Combatant Command, and other DoD components through the use of the Strategic Mission Assurance Data System (SMADS) and other available interoperable information management systems;
  - d. Identify, prioritize, and protect both physical and cyber assets deemed critical to the DON using the Mission Assurance Risk Process Model;
  - e. Periodically review and update the DON Critical Asset List. This process starts with a focus on mission and identifies those infrastructures or assets that are critical to planning, mobilizing, deploying, executing,

and sustaining military operations globally, using the Critical Asset Identification Process (CAIP); and

- f. Using the Mission Assurance Risk Management Process Model:
    - i. Conduct vulnerability and threat assessments to determine which critical assets are most at risk by considering the criticality of the asset/infrastructure, threats, vulnerabilities, and the probability of a disruptive event occurring;
    - ii. Coordinate with the appropriate mission owners in order to make an informed risk management decision;
    - iii. Prioritize remediation actions and funding requirements; and
    - iv. Monitor the progress of remediation and mitigation efforts and conduct trend analyses on all identified vulnerabilities using available automated tools such as the Core Vulnerability Assessment Management Program (CVAMP).
2. Institutionalize CIP across the Department by endorsing educational curricula, outreach, best practices and lessons learned in order to create a fundamental cultural change emphasizing the significance of DoD and DON CIP programs in ensuring mission assurance.
  3. Ensure adequate Critical Infrastructure Protection Program resource requirements are included in the Planning, Programming, Budgeting, and Execution System (PPBES).
  4. Leverage, where possible, Critical Infrastructure Protection Program applications, processes, and tools developed by other military departments and agencies in order to minimize expenditures and increase utility.
  5. Oversee the development and fielding of appropriate Critical Infrastructure Protection Program assessment and knowledge management tools as required. Coordinate with ASD (HD&ASA) and the other MILDEPS to develop and field cost effective, interoperable tools and databases.

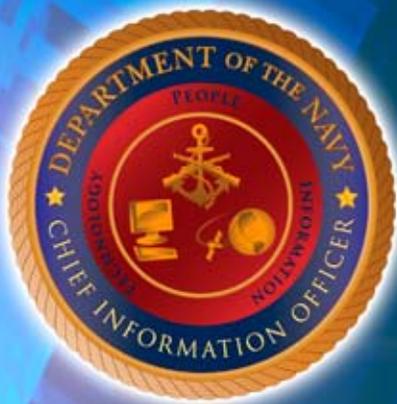
## DEFINITIONS

### **CYBER INFRASTRUCTURE**

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 all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications includes sharing and distribution of information. For example, computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

### **CYBER SECURITY**

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



# DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

1000 NAVY PENTAGON  
WASHINGTON, DC 20350-1000  
[WWW.DONCIO.NAVY.MIL](http://WWW.DONCIO.NAVY.MIL)

Department of the Navy  
Chief Information Officer

1000 Navy Pentagon  
Washington, DC 20350-1000  
[www.doncio.navy.mil](http://www.doncio.navy.mil)