DON CIP: A Comprehensive Solution to Improve Cyber and Physical Security of DON Critical Assets

By Donald Reiter, Lead for the Department of the Navy CIP Program

A primary goal of the Department of the Navy Information Management/Information Technology (IM/IT) Strategic Plan is "providing Full Dimensional Protection (FDP) that ensures Naval warfighting effectiveness." FDP involves three initiatives: Critical Infrastructure Protection (CIP), Information Assurance and Privacy. This article provides an overview on the DON CIP initiative.

What is Critical Infrastructure Protection?

CIP is mission assurance: the identification, assessment and assurance of cyber and physical assets essential to the mobilization, deployment and sustainment of U.S. military operations. Effective critical infrastructure protection identifies vulnerabilities and risks to critical assets supporting warfighting missions, remediates those validated vulnerabilities to protect against compromise, and, if compromised, minimizes impact to mission performance with effective consequence management plans and procedures.

The DON Approach to CIP

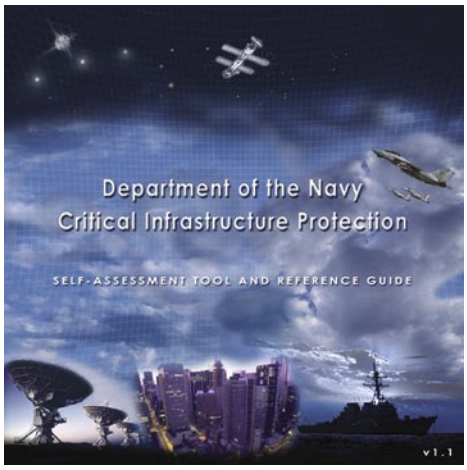
The Department of the Navy Chief Information Officer (DON CIO) was appointed the collateral duties of the DON Critical Infrastructure Assurance Officer (CIAO) in 1999 by the Secretary of the Navy to "provide a comprehensive approach to protecting the Department's critical infrastructures."

Following federal government and DoD guidance, including Executive Order PDD-63 of May 1998 and the DoD CIP Plan of November 1998, Secretary of the Navy Instruction (SECNAVINST) 3501.1 formally established DON policy, structure, and responsibilities for implementing CIP throughout the Department. The DON CIAO was given responsibilities that ranged from serving as the DON's central point of contact for CIP-related issues to sponsoring and executing a new Naval Integrated Vulnerability Assessment (NIVA) program.

The execution of these responsibilities has resulted in a fully operational, highly regarded CIP program. An independent audit commissioned by the DON CIO to assess the Department's progress concluded that "Both the DON policy and DON CIO implementation of the policy are among the best-founded and complete programs within the federal government."

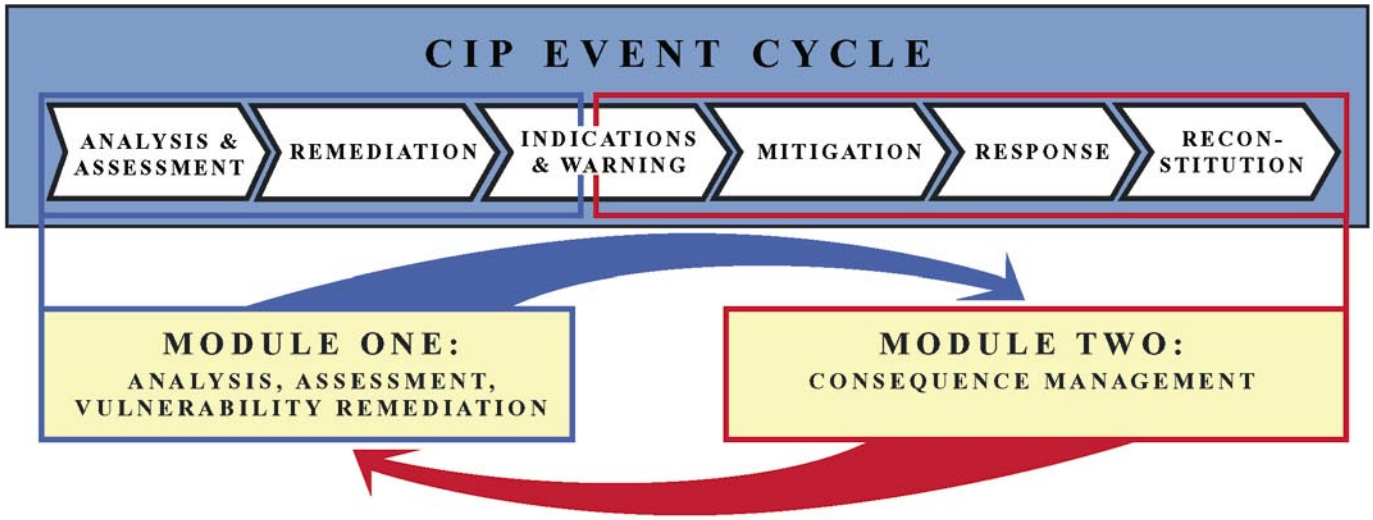
The DON CIP Initiative

The DON CIAO structured efforts around the government-recognized CIP Event Cycle (see Figure 1). This six-phase series of activities identifies actions necessary to: identify and assess critical assets, remediate significant vulnerabilities to such assets before an incident occurs, and pre-plan and maintain actions to ensure continuity of operations during and after an incident. The DON CIP Team has developed or implemented processes and tools that address all of the requirements of this event cycle (see Figure 2). A brief summary of



The CIP Self-Assessment Tool and Reference Guide enables a four-pillar assessment for those installations not scheduled for a Naval Integrated Vulnerability Assessment.

Figure 1. The CIP Event Cycle identifies activity phases essential to an effective CIP Program.



these processes and tools is provided in the following paragraphs.

DON CIP Processes and Tools

Analysis & Assessment

Naval Integrated Vulnerability Assessments (NIVA) are multidisciplined efforts involving four assessment pillars. Each pillar involves a distinct protocol and assessment focus, summarized below.

- Antiterrorism/Force Protection (AT/FP) assesses an installation's physical asset vulnerability to compromise; e.g., perimeter controls/protection, building security and guard forces.

- Computer Network Defense (CND) identifies vulnerabilities to cyber assets, e.g., computer networks, industrial controls, data retrieval and storage systems.

- Commercial Dependency (CD) assesses dependencies on off-base commercial utilities, e.g., water, telecommunications, power and transportation.

- Consequence Management (CM) planning evaluates plans and procedures that support continuity of operations throughout a disruptive event.

As illustrated in Figure 3, different organizations may be involved according to pillar and asset owner. NIVAs are conducted on installations containing DON critical assets to determine whether significant vulnerabilities exist that could jeopardize mission support if compromised. Identifying such vulnerabilities initiates a remediation and consequence management chain of events to protect those assets and assure they remain available to DON warfighters.

The DON CIAO has coordinated NIVAs in the National Capital Region, Mid-Atlantic Region, Naval District Washington, Navy Region Hawaii, Navy Region Northwest, Navy Region Southeast and Navy Region Southwest. The first NIVA outside of the continental United States (OCONUS) was conducted in October 2004 on Navy assets in Naples, Gaeta and Sigonella, Italy.

For those installations not scheduled for a NIVA, the Self-Assessment Tool and Reference Guide compact disc is available to Department personnel to enable a four-pillar self-assessment.

The Critical Asset List (CAL) is a catalog of Navy and Marine Corps assets designated as essential to the National Military Strategy. The CAL, periodically updated by the Office of the Chief of Naval Operations and Headquarters Marine Corps, influences NIVA candidate sites and allows the Department to focus limited assessment and remediation resources on assets deemed most critical.

Remediation

Remediation corrects vulnerabilites found during assessments to protect them from compromise and make them a less attractive target. The Remediation Planning Guide, published in summer 2004, provides a methodology and plan of action that assists DON entities in developing vulnerability remediation strategies that balance resources and risk. The goal is to achieve maximum return on investment while focusing limited resources on remediating the most essential assets.

Indications & Warning

The Critical Asset Management System (CAMS) is an accredited and operational stand-alone system that resides in the Naval Criminal Investigative Service (NCIS) Multi-Threat Alert Center. CAMS is the single DON CIP repository for Critical Asset List and vulnerability assessment information.

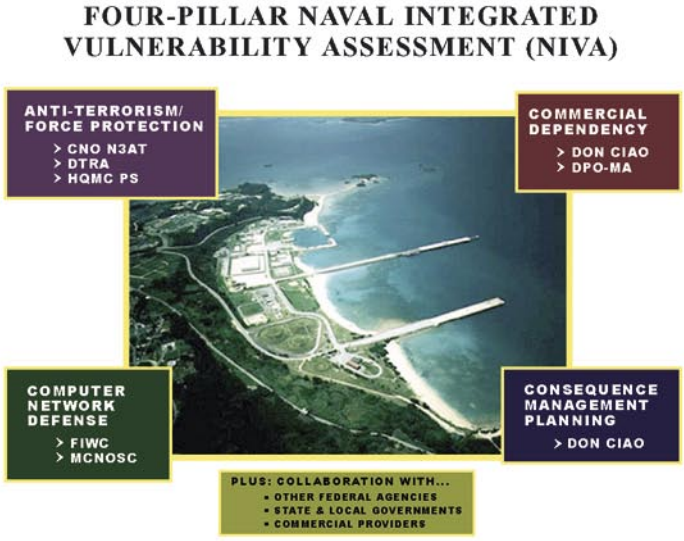
Consequence Management

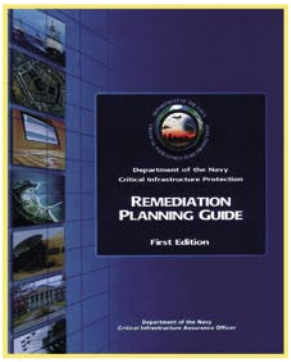
CM Assessments review how an activity's CM planning supports its overall continuity of operations. The DON CIP CM Team has reviewed over 175 CM plans since the CM pillar was added to the NIVA protocol in 2002.

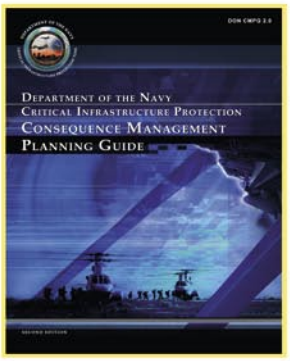
The DON CM Planning Guide (Version 2.0) provides methodology and guidance to assist CM planners with developing strategies and plans that will maintain continuity of operations during or after an event. This second edition, which has just been distributed, incorporates expanded guidance as well as information requested by first edition users.

Figure 2. DON CIP processes and tools have been developed to address the specific needs of the CIP Event Cycle.

CIP EVENT CYCLE	DON PROCESS TOOL
ANALYSIS & ASSESSMENT	✓NAVAL INTEGRATED VULNERABILITY ASSESSMENT ✓CRITICAL ASSET LIST ✓SELF ASSESSMENT TOOL ✓DEFENSE INDUSTRIAL BASE SURVEYS
REMEDIATION	✓REMEDIATION PLANNING GUIDE
INDICATIONS & WARNING	✓DON CRITICAL ASSET MANAGEMENT SYSTEM
MITIGATION	✓CONSEQUENCE MANAGEMENT PLANNING GUIDE
RESPONSE	✓CONSEQUENCE MANAGEMENT PLANNING ASSESSMENTS
RECONSTITUTION	







THE REMEDIATION PLANNING GUIDE AND THE CONSEQUENCE MANAGEMENT PLANNING GUIDE ARE AVAILABLE TO DEPARTMENT PERSONNEL ON THE DON CIO WEBSITE.

Figure 3. Naval Integrated Vulnerability Assessments look for significant weaknesses that could jeopardize mission support.

Defense Industrial Base Surveys

Defense Industrial Base (DIB) surveys review the production and delivery systems of DIB entities viewed as critical to sustaining warfighting readiness. Since 1999, 62 surveys have been completed involving DIB production of major Navy or Marine Corps weapons systems.

Based on one survey, the first commercial NIVA was conducted at a manufacturer's site. These surveys find important information and have influenced positive change in the sustainment of DON weapons systems, including establishing second manufacturing sites and moving to domestic versus foreign production.

Education and Outreach

Institutionalizing CIP throughout the DON is a primary goal implemented by education and outreach efforts. Early accomplishments include the first course on CIP presented at the Naval Postgraduate School. Recent achievements include the following initiatives.

√ The Web-based DON CIP Course is an interactive multimedia suite of instructional courseware that defines the DON CIP initiative and the roles and responsibilities of DON personnel in an effective CIP program. The four modules are categorized as Navy Courses DONCIAO-5862-1, 2, 3, 4 and Marine Corps Courses DI5500A, B, C, D.

These courses are available to Department personnel worldwide through the Naval Education Training Professional Development Technology Center (NETPDTC) e-learning and the MARINENET portals at https://www.nko.navy.mil and http://www.marinenet.usmc.mil, respectively. This course is being considered as the model for the development of a Joint Staff sanctioned course on CIP.

√ Wargame participation involves adding CIP scenarios to wargames and is an effective approach to bringing all facets of CIP to a wide audience. CIP scenarios are based on real NIVA cases in which vulnerabilities were identified.

√ Efforts to add CIP traditional schoolhouse curricula are receiving more emphasis. The most recent opportunity is the Commanding Officer Anti-Terrorism (COAT) Course given by the Center for Anti-Terrorism and Navy Security Forces at the Naval Amphibious Base, Little Creek, Va.

Also on the drawing board are the Senior Officer CIP Course for CAPSTONE, CIP Executive-Level Seminars and guest lecture briefings to DON students.

The Way Ahead

With a comprehensive program now in place, future activities will emphasize institutionalizing CIP throughout the Department.

Today's compelling challenges to mission assurance call for a proactive CIP initiative. Continuing to build on the achievements made to date and setting new goals to improve upon those measures, the DON CIP Program's focus remains firmly on the warfighters' mission assurance.

CIP Tools and Guides

The Self-Assessment Tool compact disc, Remediation Planning Guide and Consequence Management Planning Guide are available to Department personnel and are especially valuable for base commanders and installation owners.

Tools and guides are available from the DON CIO Web site at http://www.doncio.navy.mil/, then select the Products tab.

The Web-based DON CIP Courses are available to Department personnel worldwide through the Naval Education Training Professional Development Technology Center (NETPDTC) e-learning and the MARINENET portals at https://www.nko.navy.mil and http://www.marinenet.usmc.mil, respectively.

For more information, go to the DON CIO Web site at http://www.doncio.navy.mil/, the select the Products tab. CHIPS