



**Department of the Navy
Critical Infrastructure Protection**

REMEDICATION PLANNING GUIDE

First Edition

**Department of the Navy
Critical Infrastructure Assurance Officer**





DEPARTMENT OF THE NAVY
CRITICAL INFRASTRUCTURE ASSURANCE OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

25 June 2004

I am pleased to provide this Remediation Planning Guide to assist those involved with Department of the Navy (DON) remediation activities required to protect DON critical assets and support Navy and Marine Corps mission assurance.

This Guide, oriented to Base Commander/Installation Owner or the site Officer-in-Charge, has been developed by the DON Critical Infrastructure Assurance Office to serve as a tool in conjunction with the Naval Integrated Vulnerability Assessment (NIVA) and other available DON Critical Infrastructure Protection (CIP) resources to recognize, plan and enact remediation actions required to provide adequate and appropriate protection to critical assets located at DON facilities or that support DON facility mission operations. The information is structured as broad top-level guidance, with a wide variety of solutions, within which specific remediation plans can be constructed.

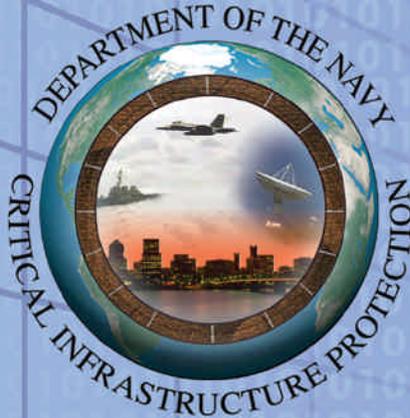
Protecting DON critical assets and assuring availability of their mission essential functions is the key tenet of the DON CIP program. Our NIVA process is a proven methodology for assessing installations, often with cooperation of state, local public and private leadership, to review in-place measures and to advise on areas of single points of failure or significant vulnerabilities. This Remediation Guide supports the next step in the CIP Cycle.

Mission Assurance is a team initiative achieved only through cooperative investment at all levels of the Chain of Command. As are each of you, I am committed to ensuring that Navy and Marine Corps warfighters can depend on the assets necessary to perform their mission. I encourage use of this Guide, and welcome any thoughts and feedback concerning its implementation or future editions.



D. M. Wennergren

**Department of the Navy
Critical Infrastructure Protection Program**



Remediation Planning Guide

First Edition

**Department of the Navy
Critical Infrastructure Assurance Officer
1000 Navy Pentagon
Washington, DC 20350-1000**

<http://www.doncio.navy.mil>



FOREWORD

The objective of the Department of the Navy (DON) Critical Infrastructure Protection (CIP) Remediation Program is to remedy vulnerabilities found in DON mission critical assets in order to protect them from failure by manmade or natural disruptive events. To support that objective, this Remediation Planning Guide provides guidance to DON personnel involved in remediating vulnerabilities to assets determined to be mission-critical to the Warfighter.

Effective remediation requires a clear process that focuses the Department's limited resources on those assets most necessary for mission success. By standardizing the process, an effective roadmap exists for all DON installations.

Significant participants in the remediation process include an Installation Owner/Base Commander or Site Officer-in-Charge; the Regional Commander for the Navy and the Bases and Stations Commanding General for the Marine Corps; and - at the headquarters level - the Commander, Naval Installations or the Marine Corps Deputy Chief of Staff, Installations and Logistics. Each must be appropriately involved during the remediation process to ensure a successful effort.

This guide identifies and discusses specific actions that are essential to remediation strategy development and implementation. Navy and Marine Corps activities, installations, commands or units should use this information as a basis from which to develop their own specific remediation approach.

This page left blank intentionally.

CONTENTS

Foreword	i
Executive Summary	v
1. Introduction	1
1.1 Key Concepts	1
1.2 Remediation in the Context of the CIP Event Cycle	2
1.3 Background	3
2. Remediation Process Tools	5
2.1 Key Personnel	5
2.2 A Disciplined Approach	7
2.3 Existing Procedures and Policy Products	8
2.4 An Informed Chain of Command	9
3. A Remediation Plan of Action	11
4. Sample Cases	15
4.1 AT/FP Vulnerability Remediation	15
4.2 Commercial Dependency Vulnerability Remediation	17
4.3 Computer Network Defense Vulnerability Remediation	19
4.4 Consequence Management Vulnerability Remediation	20
5. Conclusion	25

APPENDICES

Appendix A: Terminology	27
Appendix B: Acronyms	35
Appendix C: Remediation Timeline	37

FIGURES

Key Concepts in the Remediation Process	1
Interrelationships between the CIP Event Cycle and Remediation	2
Evolution of DON CIP	3
Full Operational Capability Solutions	4
A Disciplined Approach to Remediation	7
An Informed Chain of Command	9

This page left blank intentionally.



Executive Summary

EXECUTIVE SUMMARY

This Remediation Planning Guide has been developed to assist those involved with Department of the Navy (DON) remediation activities to develop a process to minimize or neutralize the impact of disruptive events to Naval installations – whether man-made (terrorist) or an act of nature. It is intended to serve as guidance in determining, planning, and implementing remediation actions required to protect DON critical assets and support mission assurance and sustainment.

Remediation addresses those significant vulnerabilities associated with mission critical assets that are discovered during a Naval Integrated Vulnerability Assessment (NIVA), other similar type of assessment, or a self assessment. If significant vulnerabilities are found during an assessment, an Installation Owner/Base Commander or asset owner should seek to remediate (fix) them in a prioritized fashion. An effective remediation process should address such issues as:

- ◆ The variety of methods that might be utilized... and if there is a preferred approach,
- ◆ Options that may be available to fund remediation,
- ◆ Organizations (DON and other) that can assist in remediation efforts, and
- ◆ The notification process and chain of command that must be involved.

This Remediation Planning Guide addresses these and other issues involved in establishing an effective approach and plan of action to remediate vulnerabilities. Information provided includes:

- 1. Introduction:** an overview of key terms associated with remediation and the context in which this activity is chartered and undertaken;
- 2. Remediation Tools:** a discussion of the standard elements: key personnel, a disciplined approach, available procedures and policy products, and an informed chain of command;
- 3. A Remediation Plan of Action:** six steps that should occur within an effective approach;
- 4. Sample Cases:** specific examples of possible remediation situations with associated solutions.

Because proper remediation may actually thwart or minimize the chances of a terrorist attack, it makes sense to "harden" those assets believed to be critical to the Warfighter's mission...

Remediation can provide proactive protection against criminal and/or natural acts, though different approaches may be needed depending on which type of disruption is considered. Because proper remediation may actually thwart or minimize the chances of a terrorist attack, it makes sense to harden those assets believed to be critical to the Warfighter's mission.

This guide has been developed by the Department of the Navy Critical Infrastructure Assurance Officer (DON CIAO) to serve as a tool in conjunction with Naval Integrated Vulnerability Assessments and other available resources to recognize, plan, and enact any and all remediation actions that may be required to provide adequate protection to critical assets located at DON facilities.

This page left blank intentionally.



Introduction



1. INTRODUCTION

Before discussing specific remediation tools and planning strategies, it is useful to address certain elements, relationships, and background relevant to the DON CIP Program. An Appendix of Terminology is provided at the end of this document.

1.1 Key Concepts

Reviewing several key concepts is beneficial in preparing to develop remediation strategies and plans. **Critical Infrastructure** are those physical and cyber systems needed to operate the military, government, and economy. A **Critical Asset** can be a DoD or non-DoD military-related unit, organization, installation, system, resource, equipment, or instrument identified as performing an essential function in military operational plans or support to operational plans such that it warrants measures and precautions to ensure its continued efficient operation. The Department employs a **Naval Integrated Vulnerability Assessment (NIVA)** as a primary tool to ascertain whether significant vulnerabilities and/or single points of failure exist that would jeopardize critical assets (see Figure 1-1). **Remediation** is the implementation of deliberate preventive measures before a disruptive event occurs to improve the reliability, availability, and survivability of critical assets and infrastructure. Effective remediation reduces or eliminates catastrophic impact from an attack on vulnerabilities/single points of failure, reducing the likelihood that an asset would lose mission performance capability.



Figure 1-1. NIVAs assess whether single points of failure jeopardize critical asset functionality; remediation seeks to fix such vulnerabilities.

1.2 Remediation in the Context of the CIP Event Cycle

Remediation is the second of the six activities within the CIP Event Cycle (see Figure 1-2). Defined in SECNAVINST 3501.1, the CIP Event Cycle span activities occurring before, during, and after disruptive events including hostile/terrorist acts, accidents, or natural disasters that may result

Vulnerabilities are identified within phase one - Analysis and Assessment. They are "fixed" during phase two - Remediation.

in infrastructure destruction or incapacitation. This iterative sequence of phases involves two modules: 1) activities that take place prior to an event in order to prevent occurrence or minimize impact, and 2) pre-planned actions that take place in response to an event or after it occurs. There are six phases in the CIP Cycle: Analysis and Assessment, Remediation, Indications and Warning, Mitigation, Response, and Reconstitution. Vulnerabilities are identified within phase one - Analysis and Assessment. They are "fixed" during phase two - Remediation.

The first phase begins with Warfighters and the asset owners identifying mission critical assets, specifically Tier I assets, which are those that would cause the Warfighter to suffer strategic mission failure if incapacitated.

The Department then conducts a Naval Integrated Vulnerability Assessment (NIVA) on those Tier I assets. NIVAs identify potential single points of failure that, if exploited by a terrorist or compromised by an accident or natural event, would cause the asset to fail or be unavailable and thereby threaten the success of that asset's mission. A NIVA is composed of four areas (or "pillars") of assessment: anti-terrorism/force protection, commercial dependency, computer network defense, and consequence management. Each pillar involves its own specific assessment protocol and approach.

Remediation normally occurs after single points of failure or significant vulnerabilities to critical assets have been identified during a NIVA. When assessing the vulnerabilities of an asset, the asset owner must take into account that different types of remediation actions may be necessary based on whether the cause is a criminal act (terrorist) or a natural disaster.

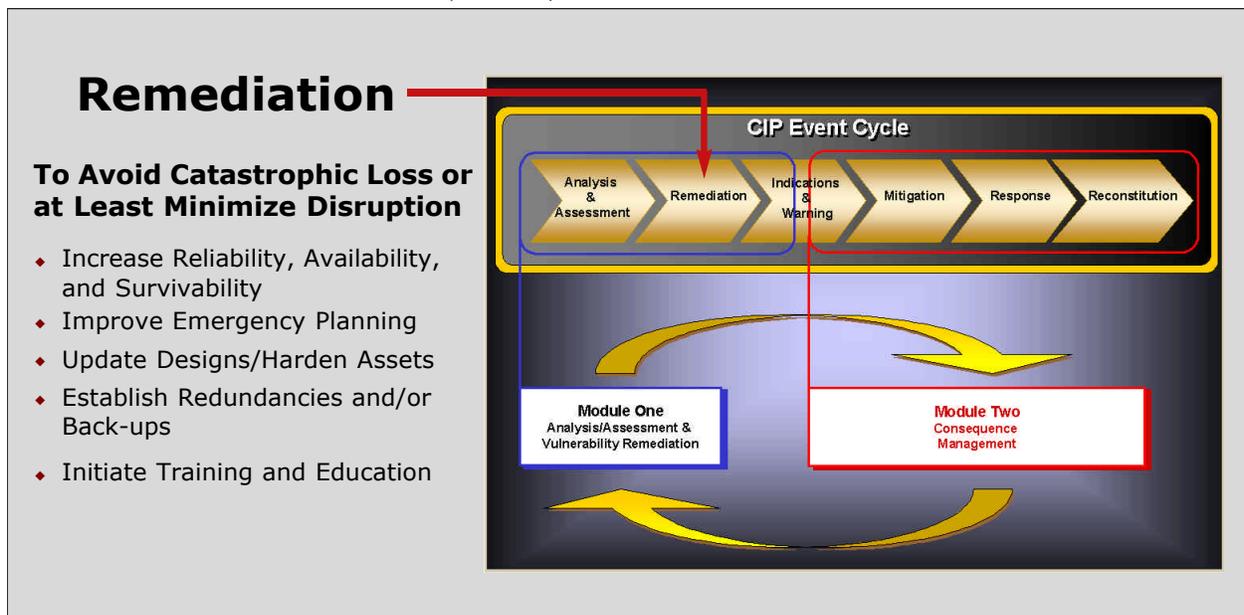


Figure 1-2. Remediation is the second phase within the CIP Event Cycle.

Remediation includes a wide range of options, including:

- ◆ Asset hardening or design improvements;
- ◆ Increased awareness, training, and education;
- ◆ Changes in business practices or operating procedures, physical diversity, deception; and
- ◆ Asset redundancy and/or back-ups.

Remediation is not limited to any one particular solution; it is taking whatever action is necessary to ensure that the critical asset will be available to the user when needed.

Remediation is not limited to any one particular solution; it is taking whatever action is necessary to ensure that the critical asset will be available to the user when needed.

1.3 Background

For many years, the need to recognize and protect the nation's critical infrastructure has been directed from the highest levels of command. Key documents have included Presidential Executive Orders such as Presidential Decision Directive/NSC-63 (now superseded by Homeland Security Presidential Directive -7) as well as guidance documents specifically from the DoD (see Figure 1-3 for a summary of primary actions associated with the evolution of the DON CIP Program).

In 1999, the Under Secretary of the Navy appointed the DON Chief Information Officer (CIO) as the DON Critical Infrastructure Assurance Officer (CIAO) and established a DON CIP Council "...in order to provide a comprehensive approach to protecting the Department's critical infrastructure." An early milestone product of the DON CIAO's Critical Infrastructure Protection (CIP) Program was the development and issuance of SECNAVINST 3501.1 of June 16, 2002, which defines DON policy and responsibilities for implementing CIP across the Department. SECNAVINST 3501.1 mandates a comprehensive program to identify critical assets and any possible vulnerabilities thereto, protect those assets from possible disruption, and - if disrupted by events - minimize adverse impact to mission performance.

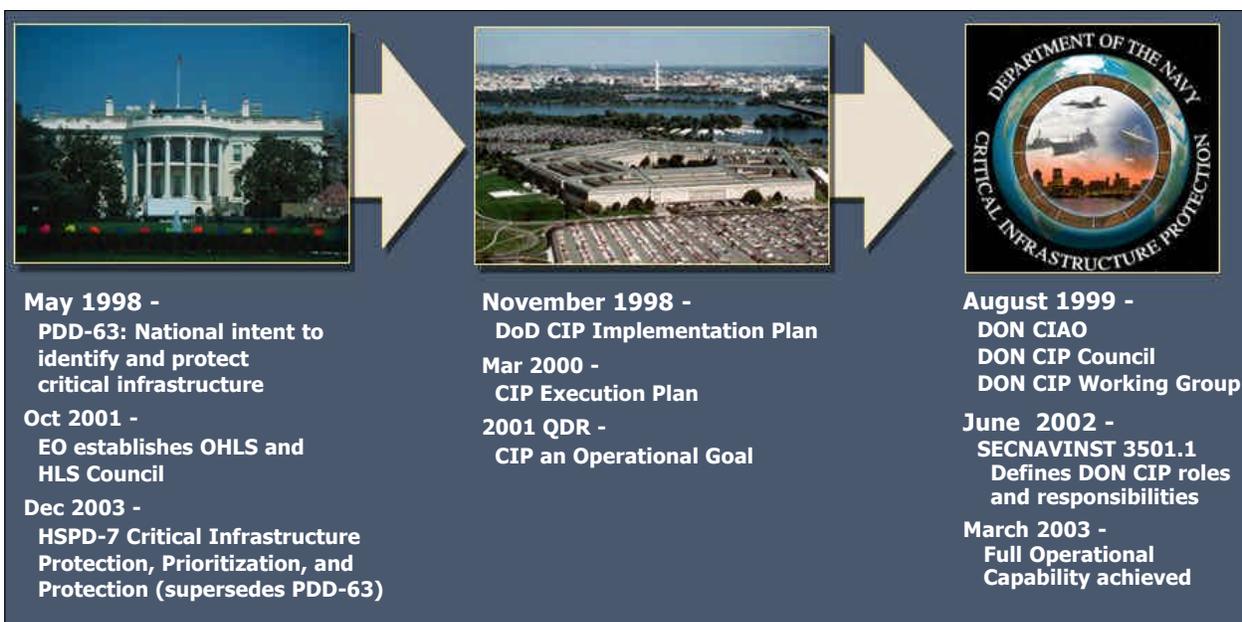


Figure 1-3. A summary of key directives in the evolution of DON CIP - from PDD-63 in 1998 to achieving a fully operational CIP Program in March 2003 (and including HSPD-7, which now supersedes PDD-63).

PDD-63 directed Federal Agencies to establish CIP operational capability by May 2003. The DON CIP Program achieved full operational capability in March 2003, having established a proven approach - including policy, implementing guidance, processes, and tools - addressing the specific needs and requirements of each of the six CIP Event Cycle phases (see Figure 1-4).

The DON CIP Program maintains an ongoing enterprise-wide initiative consistent with the current guidance provided in HSPD-7, and continues to:

- ◆ Identify physical and cyber infrastructure essential to warfighting readiness,
- ◆ Assess the vulnerability of those critical infrastructure to loss from terrorist actions or natural disasters,
- ◆ Provide vulnerability remediation guidance and strategy,
- ◆ Develop a coordinated physical and cyber indications and warning strategy, and
- ◆ Maintain consequence management efforts to ensure the continuity of DON mission essential operations should critical infrastructure be disabled.

The focus of DON CIP is to provide warfighter mission assurance. Developing and implementing effective remediation strategies and approaches are vital components of that focus.

FULL OPERATIONAL CAPABILITY	
CIP Event Cycle	Product/Service
Phase 1 Analysis & Assessment	<ul style="list-style-type: none"> ◆ Critical Asset List ◆ Defense Industrial Base Surveys ◆ Naval Integrated Vulnerability Assessment ◆ Self Assessment Tool & Reference Guide
Phase 2 Remediation	<ul style="list-style-type: none"> ◆ Remediation Planning Guide
Phase 3 Indications & Warning	<ul style="list-style-type: none"> ◆ DON CIP Data Management System ◆ I&W Strategy
Phase 4 Mitigation	<ul style="list-style-type: none"> ◆ Consequence Management Planning Guide ◆ Consequence Management Assessments
Phase 5 Response	
Phase 6 Reconstitution	
Plus	
Organization/ Program Implementation	<ul style="list-style-type: none"> ◆ SECNAVINST 3501.1 ◆ DON CIP Implementation Plan
Education & Outreach	<ul style="list-style-type: none"> ◆ Website/Training ◆ Training CDs ◆ Wargame Exercises/Regional Cooperation

Figure 1-4. Achieving Full Operational Capability signaled that the DON CIP Program offered an approach, guidance, and specific tools addressing the requirements of each CIP Event Cycle phase.



Remediation Process Tools

2. REMEDIATION PROCESS TOOLS

Certain elements are instrumental in remediation strategies and plans.

2.1 Key Personnel

■ Installation Owner/Base Commander

Once a single point of failure is identified, the first step in the remediation process is to notify the Installation Owner/Base Commander of that vulnerability. Following completion of a NIVA, the various "pillar" team leaders of the NIVA brief the Installation Owner/Base Commander and staff about the vulnerabilities discovered as a result of the assessment. In the out-brief by the NIVA team, single points of failure and/or significant vulnerabilities of mission critical assets are clearly noted. The goal is for the Installation Owner/Base Commander to have a clear assessment of what problems or potential problems were encountered and their severity. This aspect in the process will not change regardless of the type of pillar assessed (AT/FP, commercial dependency, computer network defense, or consequence management). Vulnerabilities may also be identified using the DON CIAO-developed Self Assessment Tool and Reference Guide, available to those installations not scheduled to undergo a NIVA (or for use between NIVAs). Vulnerabilities identified using that tool would be addressed using the same remediation process as if found during a full-up NIVA.

■ Key Personnel Resources for the Installation Owner/Base Commander

Depending on the types of vulnerabilities encountered, other personnel should be notified and/or consulted to work through remediation. The particular individual(s) to be consulted depends on the scope and nature of the vulnerability and NIVA pillar(s) involved. The following paragraphs list (in alphabetical order) those most likely to be contacted and the types of issues each would normally handle.

◆ Commander, Naval Installations (CNI) Staff

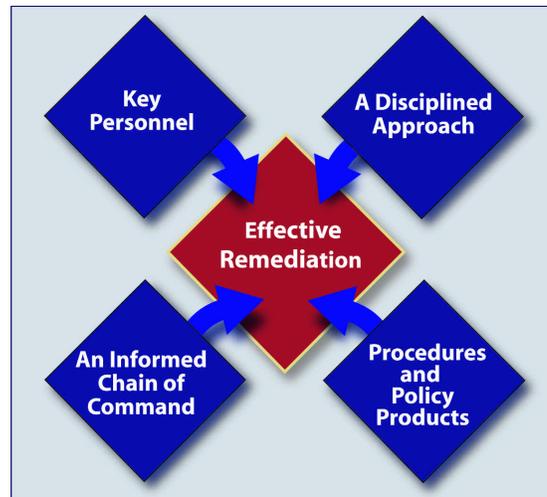
Representatives of the CNI staff may be contacted, as appropriate, concerning issues of long term installation construction, consolidation, funding and budgeting process when dealing in the areas of Base Support, Operating Forces Support and Community Support.

◆ Contracting Officer

The Installation Owner/Base Commander can contact the Contracting Officer to resolve/investigate commercial dependency vulnerabilities. This type of remediation could range from contracting with other more reliable commercial enterprises or making arrangements for alternative sources for the commercial product.

◆ Critical Infrastructure Protection (CIP) or AT/FP Officer

This person is a primary point of contact for "inside the gate" physical issues, similar to the base Security Officer. Vulnerabilities associated with the physical security of the installation include fencing, security lighting, security training, the security guard force, physical barriers, entry control points, and other physical security elements dealing with the integrity of the installation.



◆ **DON CIAO Staff**

Members of the DON CIAO staff are available to discuss remediation options.

◆ **Engineering Field Personnel**

Engineering Field Personnel (EFP) can be engaged by the Installation Owner/Base Commander when engineering techniques are remediation options. Such techniques could be anything from re-engi-

neering an existing asset to creating a redundant capability to lessen a single point of failure/vulnerability. While this would most likely apply to those vulnerabilities discovered for commercial enterprises supporting the installation, EFP could also be used for certain "inside" the gate issues.

KEY PERSONNEL RESOURCES INCLUDE

- ◆ **Installation Owner/Base Commander**
- ◆ **Commander, Naval Installations Staff**
- ◆ **Contracting Officer**
- ◆ **CIP and/or AT/FP Officer**
- ◆ **DON CIAO Staff**
- ◆ **Engineering Field Personnel**
- ◆ **Information Systems Security Officer**
- ◆ **Officer-in-Charge, Commander Naval Networks & Space Operations Command**
- ◆ **Public Works Officer**
- ◆ **Regional Commander's Staff**
- ◆ **Security Officer**

◆ **Information Systems Security Officer**

The Commanding Officer has the ultimate responsibility to ensure the integrity and security of legacy computer networks. However, the CO would rely heavily on the Information Systems Security Officer (ISSO) to ensure that computer network vulnerabilities discovered in the course of a NIVA are remediated. The ISSO would most

likely assign the actual remediation action to the System Administrator(s) to execute, but should a vulnerability require resources beyond the Command's control, the ISSO would prioritize efforts and establish and prepare a budget and timeline required for achieving the remediation necessary to reduce or eliminate the threat posed by the vulnerabilities identified.

◆ **Officer-in-Charge, Commander Naval Networks and Space Operations Command**

In the case of a network that has come under control of the Navy & Marine Corps Intranet (NMCI) (from Assumption of Responsibility (AOR) through full cut-over), the responsibility to address vulnerability remediation rests with the geographic Network Operations Center (NOC). The government representative to the contractor for NMCI at each NOC is the Officer-in-Charge, Commander Naval Networks and Space Operations Command (OIC CNNSOC) Detachment. The OIC and the Detachment Staff should be the primary conduit to address Base/Command/Installation vulnerability remediation under NMCI and should be included in any Command's plan of action in addressing remediation of CND vulnerabilities.

◆ **Public Works Officer/Staff Civil Engineer**

The Public Works Officer (PWO) can be engaged for any number of both "inside" and "outside" the gate vulnerability issues. In most cases, PWOs become involved when a vulnerability has been discovered in one of the commercial assets that the base depends on to accomplish their mission. Examples of these commercial dependencies include: electric power, telecommunications, natural gas, roads, railways, waterways, and any other services provided by a commercial vendor in support of a Naval installation. Normally, the PWO will already have many contacts with each of these commercial enterprises, and will be able to negotiate with these enterprises on behalf of the Installation Owner/Base Commander.

◆ **Regional Commander's Staff**

Representatives of the Regional Commander's staff may be involved, as appropriate, in the remediation process at the Installation Owner/Base Commander level depending on the significance or type of vulnerability under review. Frequently, Remediation Plans, including those requiring additional funding, budgeting and resources, will be reviewed/approved at the region prior to forwarding to CNI.

◆ **Security Officer**

In many cases, this Officer will also be the CIP or AT/FP Officer. Therefore, vulnerability remediation issues within this individual’s purview will be similar to those described under "CIP or AT/FP Officer." These individuals usually deal with vulnerabilities discovered inside the gate.

2.2 A Disciplined Approach

The Installation Owner’s/Base Commander’s team should initially determine which vulnerabilities involve the most important mission critical assets and focus their remediation efforts on those vulnerabilities first. Lower priority vulnerabilities can either be remediated last or possibly not at all if they do not rise to a level that would adversely affect mission essential functions. Usually, there are multiple solutions to any remediation problem. For example, improving the reliability, availability, and survivability of mission critical assets and infrastructure may be accomplished in ways including:

- ◆ Changing business practices/operating procedures,
- ◆ Increasing awareness and training,
- ◆ Graceful system degradation & priority restoration,
- ◆ Emergency planning for electrical load shedding,
- ◆ Asset hardening or design improvements, and
- ◆ System level changes such as physical diversity, deception, and redundancy.

Figures 2-1 and 2-2 illustrate a structured approach to evaluating a wide array of options. Each focus area in Figure 2-2 below lists typical subject areas that should be addressed to ensure the highest potential for successful remediation.

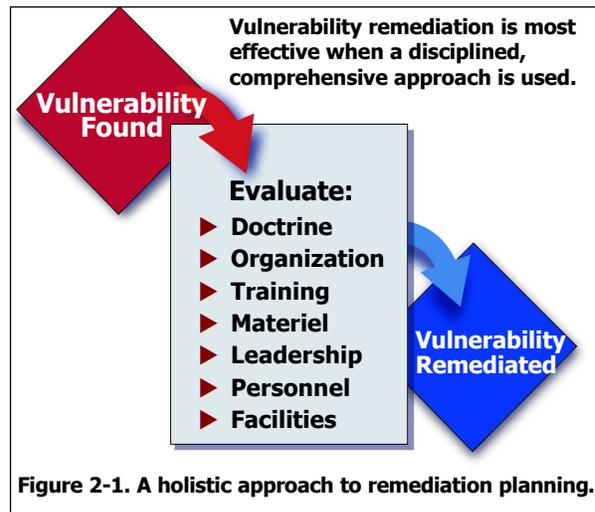


Figure 2-1. A holistic approach to remediation planning.

Identify, organize, and integrate a wide range of solutions.

<p>1) DOCTRINE. What policy doctrinal changes might reduce the impact of the vulnerability? Possible options include:</p> <ul style="list-style-type: none"> - Local Policies - Procedures - Agreements (MOUs, ISSAs, etc.) 	<p>4) MATERIEL. Possible options include:</p> <ul style="list-style-type: none"> - Physical - Cyber - Access - Redundancy
<p>2) ORGANIZATION. How can changes to the organizational structure reduce the impact of the vulnerability? Possible options include:</p> <ul style="list-style-type: none"> - Structure - Location 	<p>5) GOVERNANCE. Possible options include:</p> <ul style="list-style-type: none"> - Centralized - Decentralized
<p>3) TRAINING. How may training (new or improved) reduce the vulnerability's impact ? Possible options include:</p> <ul style="list-style-type: none"> - Formal - Informal - Situational Awareness 	<p>6) PERSONNEL. Possible options include:</p> <ul style="list-style-type: none"> - Government - Contractor - Third Party - Full- or Part-time
	<p>7) FACILITIES. Possible options include:</p> <ul style="list-style-type: none"> - Physical - Access - Security

Figure 2-2. Typical subject areas addressed within a comprehensive approach.

Example:

Commercial Power Reliance and Subsequent Vulnerability

ISSUE: An installation is totally reliant on commercial power. The commercial power enters the base through a single point of entry and the entire base is on one circuit. By disabling that single point of entry, a terrorist could cut all power to all functions (critical and noncritical) on that base.

POSSIBLE SOLUTIONS to this vulnerability, using the aforementioned holistic approach.

- 1) **Doctrine:** Are there changes in policy or processes that would allow a back-up or secondary source of power? It may be feasible to develop a plan that shifts critical functions to another installation if the power goes out for more than three hours.
- 2) **Organization:** Are there options involving organizational or location changes? Yes, if it is possible to locate the critical functions requiring power at a neighboring installation that does not have the same vulnerability.
- 3) **Training:** How might training alleviate the single source aspect? If a decision is made to provide back-up capability with emergency generators, train designated personnel in their operation.
- 4) **Materiel:** What procurement requirements result from option analysis? If the emergency generator is a solution, procure an emergency generator; install an Uninterruptible Power Supply (UPS) to support power to the critical functions while the utility company restores power.
- 5) **Governance:** Does the vulnerability require a top-level decision-making process? It may be that the best remediation is deciding that the installation will not rely on commercial power sources at all for certain critical functions.
- 6) **Personnel:** It may be necessary to hire a generator operator/mechanic to operate an emergency generator. Options include Government or contractor personnel, full or part-time.
- 7) **Facilities:** Depending on the remediation solution selected, options might include: establishing an agreement with the utility company for a second source of power to the installation and/or for a high-priority restoration of power to the installation; contracting for the placement of an emergency generator to power critical function(s), including a service agreement to maintain that generator and fuel to sustain that generator.

Planners must conduct an analysis to determine how the proposed action(s) impacts the installation that enacts the remediation action. In the example above, the cost of having a priority recovery for the utility aboard the installation should be determined, as well as the cost to procure, staff, and utilize an emergency generator.

2.3 Existing Procedures and Policy Products

While it would be impossible to describe every type of solution for every type of vulnerability, there are some basic remedies evolving from this approach that will fit many scenarios. The following "solutions" are examples of actions that cover a wide range of options appropriate for many situations.

■ Memorandum of Understanding or Agreement (MOU/MOA)

MOUs/MOAs can be used between the Installation Owner/Base Commander (or as deemed appropriate) and civilian agencies or other DoD entities to provide physical security of certain mission critical assets. For example, a building that has been designated as a mission critical asset might be located at the edge of a military base and close to an unprotected civilian

area. An MOU/MOA could be arranged with local law enforcement authorities to increase patrols in that area during periods of increased threat to provide more security. This same technique could be used with other civilian and DoD agencies to increase protection. The main thrust of this technique is collaboration with other DoD and non-DoD agencies to ensure protection of mission critical assets, and it is a relatively inexpensive approach.

■ **Base Support**

In some remediation situations, an Installation Owner/Base Commander, with the support of the Regional Commander and CNI, would provide resources for solutions such as fencing, lighting, barriers, or other physical security measures to reduce the risk of a terrorist attack that are above what their normal budgets could support. For example, the Installation Owner/Base Commander could erect fencing around a building housing a mission essential function to provide more security or could install lighting in key areas to illuminate the building at night. Parking could be relocated to provide a larger "blast" area to counter use of explosives via automobile. Or, all of these measures could be employed to increase the survivability of the building.

■ **Program Objective Memorandum (POM)/Supplementals**

The POM process is one primary source of funding in cases where significant amounts of funding or manpower are required to remediate the vulnerability. In such cases, the Installation Owner/Base Commander should request funding to do so through the appropriate chain of command (e.g., request CNI/Region support remediation funding in documents heading to POM). This action is appropriate in those instances where a Tier I mission critical asset requires significant funding to correct a problem that if exploited, would prevent or seriously degrade the Warfighter's ability to wage war. This remediation approach would usually involve significant time and funding such as that planned for and resourced in the POM. For example, an entire redundant facility may have to be built to compensate for the potential destruction of the primary facility, or the facility function might have to be relocated to a building much more hardened via the use of Military Construction (MILCON) Appropriations.

2.4 An Informed Chain of Command

Once the mission critical asset vulnerabilities have been identified and the remediation solutions planned or accomplished, the appropriate chain of command should be notified. This involves not only the Installation Owner's/Base Commander's immediate chain of command, but it should also include a report via the appropriate service to the DON CIAO. As illustrated in Figure 2-3, significant participants include Commander, Naval Installations (CNI); HQs Marine Corps Installations and Logistics (I&L); Navy Regional Commanders and USMC Bases/Stations Commanding General (CG). When remediation solutions are relatively simple/inexpensive, they should be scoped, estimated, prioritized, and reported appropriately as soon as possible. When remediation appears to be complex, expensive, and/or requires significant time/manpower, the chain of command should be notified of the plan of action. Notifying higher authorities ensures that everyone who needs to know will be aware of efforts in progress.

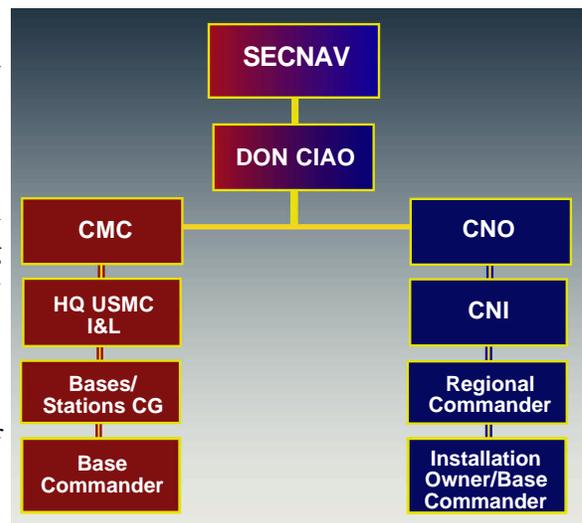


Figure 2-3. Successful remediation involves an informed chain of command.

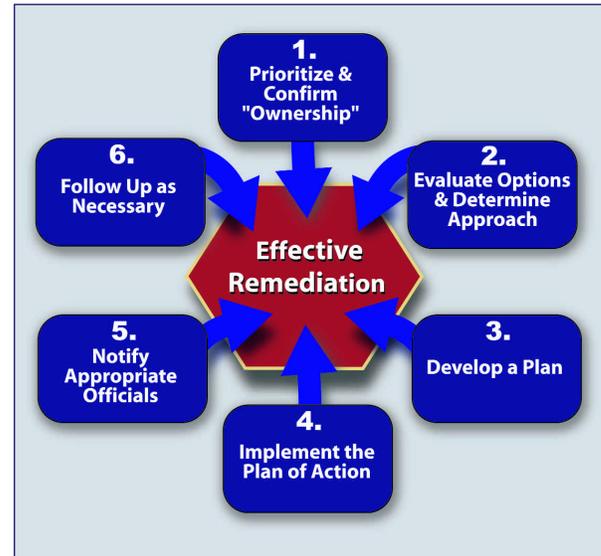
This page left blank intentionally.



Remediation Plan of Action

3. A REMEDIATION PLAN OF ACTION

Basic steps apply to all remediation efforts after single points of failure have been identified.



3.1 Basic Steps to an Effective Plan

Step 1: Confirm "Ownership" and Prioritize Vulnerabilities

TIMEFRAME: as soon as possible after identification of single points of failure

Specific actions within this first step should include the following:

- ◆ **Identify/confirm who controls or owns the mission critical asset**

During this first step in the process, it is important to know who the "responsible officials" are so that those most relevant can be brought into the process early (see Section 2 discussion on engaging responsible officials). Form a remediation team of key participants based on the types and areas of vulnerability to be addressed. For example, to remediate a vulnerability in physical security, one key participant would probably be the Installation Owner/Base Commander, among others. To remediate a vulnerability that involves a commercial utility, Navy Bases would engage the local Naval Facilities Engineering Command (NAVFAC) component, USMC Bases would contact the Headquarters Marine Corps Deputy Commandant, Installations and Logistics (I&L), to take advantage of their contractual relationship with that provider. In some cases, though, the commercial enterprise (e.g., power or telecommunications company, water provider, rail line, etc.) may willingly support changes that can remediate the problem.

EXAMPLE: To remediate a vulnerability that involves a commercial utility, Navy Bases would need the local ... NAVFAC component, USMC Bases the Deputy Commandant ... I&L group, to take advantage of their contractual relationship with that provider. In some cases, though, the commercial enterprise (power company, telecommunications company, water provider, rail line, etc.) may willingly support changes that can remediate the problem.

- ◆ **Prioritize all single points of failure found in order of importance**

As noted earlier, an important step is to determine which vulnerabilities involve the most important mission critical assets and focus the remediation efforts on those vulnerabilities first.

Step 2: Analyze Options and Determine the Best Approach

TIMEFRAME: ideally, within 30 days after receiving NIVA reports or identifying significant vulnerabilities

- ◆ **Evaluate options; determine those most logical, cost effective, and likely to prevent either a terrorist attack or other disruption of service**

No remediation strategy is likely to provide 100% protection against attack. A more realistic goal is to identify and implement protective/corrective options that achieve either an avoidance of an attack or graceful degradation in systems and assets should an attack occur. In addition to identifying realistic goals, an important consideration is the array of "costs" usually involved to implement a remediation option. Such costs are not just monetary; they also include:

- Time required to implement the remediation,
- Manpower to execute the plan, and
- Impact the remediation effort may have on the relationship between an installation and the surrounding civilian community.

Option analysis must balance risk vs cost vs mission assurance. An effective approach is the "Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities" process described in Section 2.2. The use of such a disciplined and comprehensive checklist enables planners to identify, organize, and integrate as broad a range of solutions as possible. (The Case Studies provided in Chapter 4 illustrate various thought processes and strategies that might be used within sample vulnerability situations.]

Step 3: Develop the Remediation Plan

TIMEFRAME: as soon as practicable, but no longer than 60 days after the NIVA

It is important to emphasize that remediation does not necessarily mean physical alteration of the single point of failure. Rather, it includes any preventive action that lowers the probability of a successful terrorist attack against a given mission critical asset. Options are broad and can range from such actions as executing a physical remedy (e.g., improved stand-off barriers), to procuring additional assets (e.g., generators for power), to entering into agreements to protect an asset with security forces at heightened threat conditions, to education and training.

- ◆ **Develop a plan of action and milestones (POA&M) focusing on the actions chosen to remediate the problem**
- ◆ **Detail what needs to be done, how it will be done, who is involved, and when the remediation action should be complete**
- ◆ **Forward a copy of the Remediation Plan to the DON CIAO via the appropriate chain of command**

Step 4: Implement the Plan of Action

TIMEFRAME: within 2-4 weeks of Plan approval

Once all approvals have been received and issues such as manpower and schedule are in line, remediation action commences. Appropriate officials should be engaged in the process as necessary.

Step 5: Notify Appropriate Officials

TIMEFRAME: at Plan commencement and within 2-4 weeks of Plan completion

- ◆ **Notify appropriate Senior Officials, including the DON CIAO, once remediation has begun and again at completion**

At Plan execution, all Senior Officials, including the DON CIAO, should be notified that remediation has begun. In addition, once the Plan is completed, these same officials should be notified within 15 days. As applicable, one year after receipt of the NIVA report(s), a status report should be submitted to all concerned parties addressing the remediation efforts to date, and, if remediation efforts have not been completed, an estimate of when they will be.

Step 6: Execute Follow-Up Actions

TIMEFRAME: three years after a NIVA

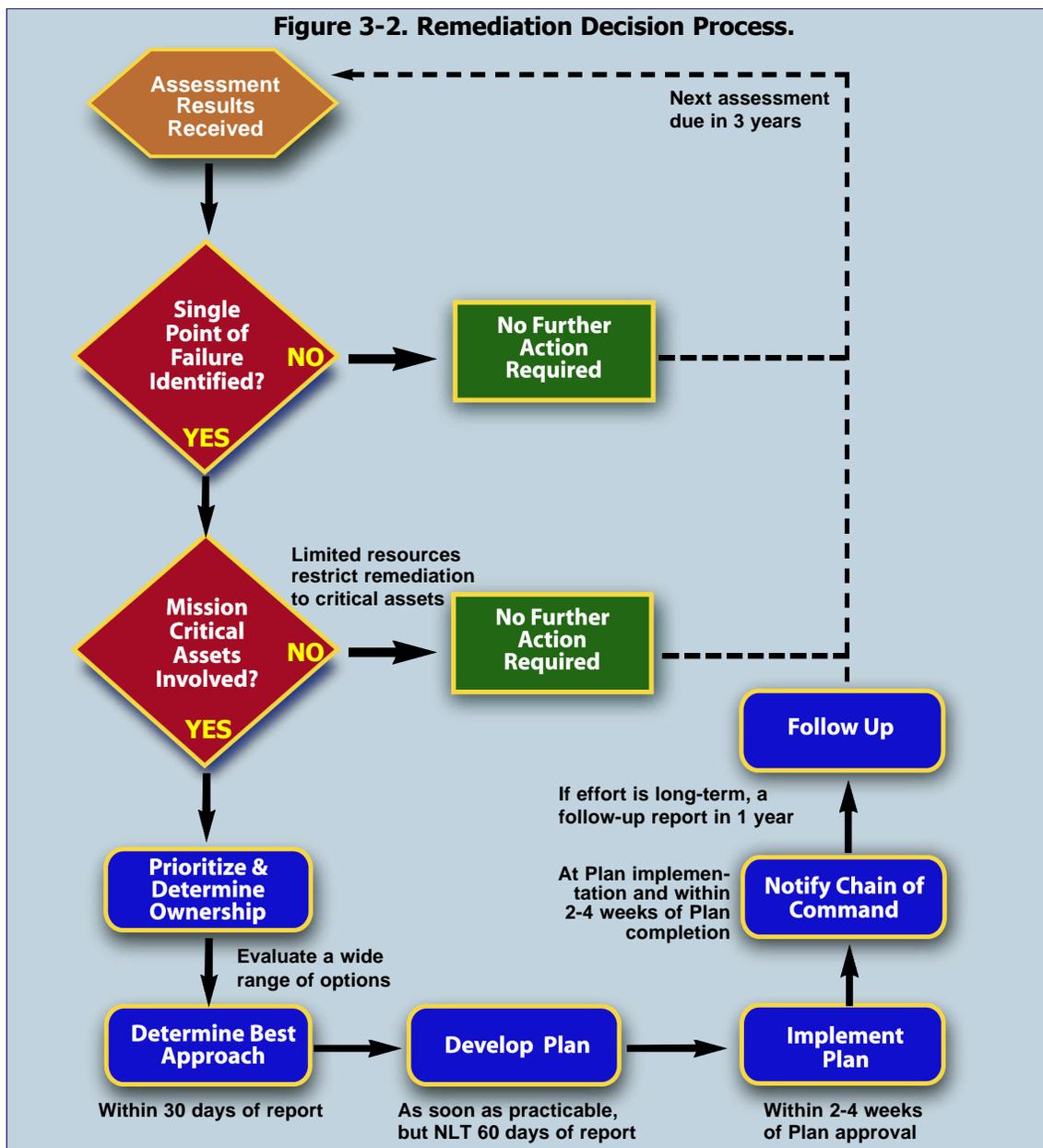
Three years after a NIVA has been completed on a mission critical asset, another NIVA should be scheduled to keep critical asset protection awareness current. NIVA coordination should be handled through the Service Headquarters and the DON CIAO. In the interim, Installation Owners/Base Commanders have the option of using the DON CIP Self-Assessment Tool and Reference Guide to continue to assess their installation for any potential single points of failures or other significant vulnerability.

3.2 Summary View of the Remediation Process

Assessment of mission critical assets is an iterative process. A summary of the process is provided below in Figure 3-1. Figure 3-2 illustrates a generic remediation decision-making process. It should be noted that an Installation Owner/Base Commander can request a special NIVA at any point in time if there is reason to believe that a mission critical asset or other similarly important considerations have changed significantly. For example, a mission critical asset may have been added to a base since the last assessment. In that case, a NIVA should be conducted to determine whether significant vulnerabilities exist.

Action	Description	Due	Submit to
Analyze Findings (NIVA)	Determine mission critical single points of failure	Within 30 days after receipt of assessment report	Installation Owner/ Base Commander
Develop a Remediation Plan	Develop POA&M to remediate single points of failure	As soon as practicable but no longer than 60 days after assessment	Installation Owner/ Base Commander and DON CIAO
Implement the Plan	Commence plan to remediate vulnerability	Within 2-4 weeks after approval of Plan by Chain of Command	N/A
Notify the Chain of Command	Written report detailing remediation effort	At commencement and within 2-4 weeks after Plan completion	Chain of Command and DON CIAO
Follow-Up	Schedule follow-up assessment	3 years after last assessment	Coordinate with Service Headquarters and DON CIAO

Figure 3-1. A Summary Overview of the Remediation Process.



■ **The Remediation Decision Process**

Figure 3-2 illustrates that action is pursued only when a single point of failure is found that involves a mission critical asset. Whether an asset is “mission critical” is driven by that installation’s mission essential functions (MEFs). SECNAVINST 3501.1 defines mission essential as any asset or function that is vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. MEFs are those specific functions necessary to sustain the minimum operational processes that generate the critical asset’s contribution to a given Operational Plan. Infrastructure is considered critical only if it supports a mission essential function. Figure 3-2 illustrates that “no further action” is required if a single point of failure does not involve a mission critical asset. Limited resources (funding and manpower) available for remediation require that Installation Owners/Base Commanders determine that a mission critical asset is impacted before proceeding, and if so, to prioritize remediation efforts if more than one significant point of failure exists to such an asset.



Sample Cases

4. SAMPLE CASES: EXAMPLES OF VULNERABILITY REMEDIATION WITHIN THE FOUR NIVA PILLARS

Brainstorming as many options as possible for remediating any single point of failure is a good approach for arriving at the best solution for that specific situation. This section provides examples of vulnerabilities and the options that could be derived during a subsequent remediation decision-making process. One obvious remediation approach would be to duplicate the mission essential functions at a separate location; however, a thorough evaluation would likely provide a less costly solution in many cases. The examples provided are in the context of the four NIVA pillars: AT/FP, Commercial Dependency, Computer Network Defense, and Consequence Management.



4.1 AT/FP Vulnerability Remediation

The assessment of physical and/or personnel security areas is often called an anti-terrorism/force protection (AT/FP) assessment. In a broad sense, it is a look at the physical/personnel security and associated training that a facility utilizes to maintain both protection of critical infrastructure and a safe environment for installation personnel and their families.

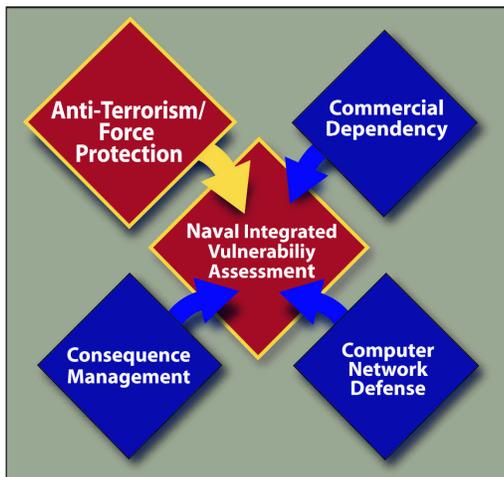
■ AT/FP Vulnerability: WATERBORNE ATTACK

Vulnerability: A recent NIVA aboard a Naval Station discovered that the base is particularly vulnerable to waterborne attack because of the poor lighting, lack of fencing, and other security related measures near the piers. When there are no ships present, there is virtually no security provided to the area adjacent to the water.

Remediation: There are several methods for remediating this vulnerability. Fencing could be placed around the perimeter of the harbor to prevent unauthorized personnel from boarding the Naval Station. Security patrols could be increased to monitor the area adjacent to the water, and lighting could be installed to illuminate the area. In the event the assets to be protected are mission critical assets, motion detectors could be installed on the grounds to alert security personnel. Canine patrols could also be employed to further secure the area. The level of remediation will depend on the level of risk that the asset owner or Installation Owner/Base Commander is willing to assume.

■ AT/FP Vulnerability: BUILDING SECURITY

Vulnerability: A high level Naval Education Institution aboard a Naval Station allows anyone who has successfully gained access to the facility to park under the institution in an underground garage. There are no gate passes or other ingress points involved to access this below ground parking. Furthermore, during certain periods of night, the gates to the Naval Station are



not guarded. While the entrance to the underground parking facility will not allow access by a truck over the height of six feet/six inches, it will nevertheless allow access to anyone who has successfully accessed the Naval Station. This institution is often occupied by senior military personnel from all branches of the DoD, senior civilians, and senior foreign military officers. Because of political pressures, security is maintained at its lowest level. The result is that the building is susceptible to a car bomb in the underground parking facility. This situation is further aggravated by the building being located right next to a large bay of water, allowing a potential terrorist many avenues of escape.

Remediation: As is the case with most vulnerabilities, this can be remediated in a number of ways. First, a security system could be installed that would require users of the underground parking lot to use an entrance card to access the facility. The gates could be alarmed so that in the event the gate is charged by a vehicle an alarm is activated which notifies security personnel and that causes an automatic barrier to appear that would prevent the vehicle from entering the facility. If this is not feasible for funding or political reasons, security could be enhanced at the Naval Station gates to better scrutinize entrants to the base. Waterborne security could also be enhanced to provide better protection from the bay side. Further, another perimeter fence could be established around the educational institution inside the Naval Station's perimeter fence to allow yet another barrier for entrants to transit. During an extremely high terrorist threat level condition, people could be completely barred from parking in the underground parking facility. This would at least ensure that no explosive-laden vehicle could access the underground parking area.

■ **AT/FP Vulnerability: BRIDGE ACCESS TO BASE**

Vulnerability: A NIVA conducted aboard a USMC Base determined it to be located on an island that houses several mission critical assets. The only access to this island and the Base is via one bridge from the mainland to the island. Additionally, several utilities use this bridge to transit the waterway via various conduits. These utilities are electrical power cables, a large, commercial water pipe, and telecommunications cables. Destruction of this bridge would be a single point of failure for the successful operation of the Base and the mission critical assets thereon. Loss of this bridge would essentially halt operations aboard the Base.

Remediation: There are a number of ways to remediate this vulnerability. Some require great expense, while others are relatively inexpensive. One method of remediation would be to build a second bridge to the island with redundant capability including the various utility connections that cross the bridge. While this would certainly fix the vulnerability, it would be extremely expensive and time consuming. Another alternative would be to place the utility cable conduits underground and underwater to ensure that the Base maintains its connectivity to these commercial enterprises. As far as the disruption of transportation across the bridge should it be destroyed, arrangements could be made prior to any problem to have a ferry boat transport people, vehicles and supplies to the island. Again, this would be very expensive. The most inexpensive method of remediation might be to establish an MOU with the local law

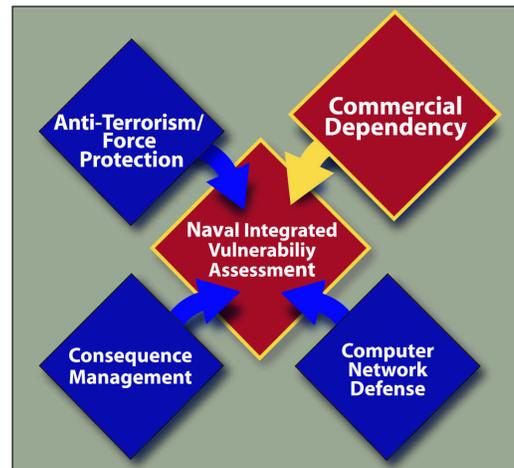
enforcement authorities who will assist in protecting the bridge during heightened terrorist threat conditions. This could be further enhanced with Base security personnel to ensure that security is placed on and around the bridge 24 hours a day during times of heightened tensions. While none of these remediation techniques provide a 100% guarantee that the bridge and the accompanying utilities would always remain intact, they would increase the probability of survival compared to doing nothing.

4.2 Commercial Dependency Vulnerability Remediation

DoD installations may rely heavily on commercial services, and loss of their services could have a huge impact on mission assurance. The impact that commercial entities have on the success or failure of the DON's mission require it to be a pillar in the NIVA process.

The remediation of vulnerabilities posed by commercial dependency is not as easy to accomplish as those posed by DON owned infrastructure. Liaison between the DON facility and the commercial service provider should have occurred before the assessment and remediation phase. Any rapport established certainly aids in any required remediation. Efforts to perform remediation with commercial services should be coordinated through the facility's Public Works Officer, Contracting Officer, Public Affairs Officer, or other relevant personnel on the installation as appropriate.

Approaching the remediation of vulnerabilities from commercial dependencies vary from situation to situation. Three examples of such vulnerabilities and ways to remediate them are provided below.



Examples of Commercial Services Used by DoD

Electric Power
Water
Natural Gas

Transportation
Telecommunications
Oil

■ Commercial Dependency Vulnerability: FUEL PUMPING STATION

Vulnerability: A NIVA conducted aboard a Naval Installation determined that a JP-5 pipeline pumping station was vulnerable to terrorist attack. While the pipeline was underground both on and off the Naval Installation, the pipeline goes above ground at the point where it connected to an intermediate pumping station. It was at this point that the pipeline was most vulnerable to attack and destruction. The NIVA discovered that destruction of this pumping station would completely stop all JP-5 fuel from entering the base. This would, in turn, greatly affect the mission capability of both ships and aircraft aboard the Naval Installation. This was the only fuel pipeline that provided JP-5 fuel to the base.

Remediation: There are several ways to remediate this vulnerability. First, a high, chain-link fence could be built around the pumping station with enhanced lighting to prevent easy access to the pumping station. This would provide some security for the pumping station although it would

probably not be adequate enough to prevent a terrorist attack. Second, by previous arrangement, the pumping station could be guarded during a time of heightened security threat conditions by contracting with a private security company. Third, arrangements could be made in advance of any threat or terrorist attack to have JP-5 fuel transported to the installation via trucks, barges or rail. While this would not necessarily replace the pipeline, it would continue the fuel capability of the installation in support of operating forces. Fourth, another JP-5 fuel pipeline could be constructed to provide redundant fuel access, although this would probably be the most expensive option available. Lastly, arrangements could be made to have the ships and aircraft transit to another nearby Naval installation to gain access to JP-5.

■ **Commercial Dependency Vulnerability: TELECOMMUNICATIONS**

Vulnerability: A NIVA of a Naval Installation determined that local and long distance telecommunications nodes were co-located in the same building just outside the confines of the base. According to NIVA data, if terrorists destroyed this building, all local and long distance telephone traffic would be disrupted for the entire Naval Installation. This disruption could adversely affect the mission essential operations aboard the Naval Base.

Remediation: The most logical first step to remedy this situation would be to contact the local telecommunications provider to determine what redundant capabilities might exist to continue service should the building where the two nodes are located be destroyed. The telecommunications provider might be able to re-route traffic through another telecommunications node to the Naval Installation to continue uninterrupted service. Next, the local telecommunications provider could identify portable and temporary service equipment that could be used to provide the Naval Installation with continued service. Another means of remediation would be to ensure that all key base personnel had cellular telephones. This would enable them to continue to communicate with necessary on-base and off-base personnel despite the loss of regular land-line services.

■ **Commercial Dependency Vulnerability: ELECTRICAL POWER**

Vulnerability: A single electrical power substation provides all of the electric power requirements to a Marine Corps Installation, which has a concentration of mission critical assets. These mission critical assets demand electric power to function. This particular electrical power substation is just outside the perimeter of the Marine Corps Base, and, except for a chain link fence, it is virtually unprotected. There is a small road leading to this electric power substation from a major thoroughfare. Shortly after turning onto the small road from the major thoroughfare, a locked "pole" barrier blocks the small road from anyone who is not an authorized electric power company official possessing a key to the barrier. However, examination of the immediate area surrounding the "pole" barrier disclosed that circumventing the barrier would be easy in a four-wheel drive vehicle or motorcycle. This would then make it possible for a terrorist to drive a car or truck bomb near the perimeter of the power substation and destroy it, rendering it inoperable and eliminating all base electric power.

Remediation: The following remediation options are just some of the options available to the Marine Corps to fix these vulnerabilities. One, they could arrange to have large diesel generators delivered to the base to provide electric power until the power substation was repaired or

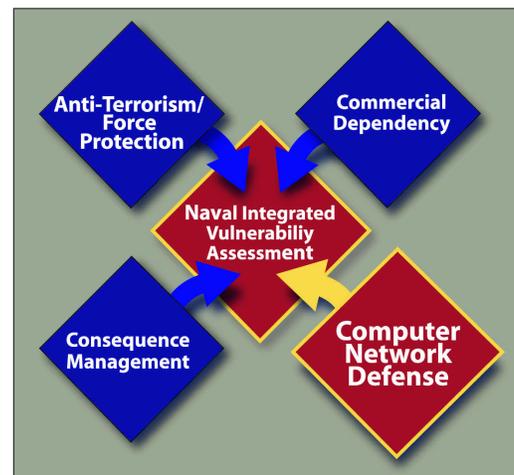
electric power was established by some other means. Two, they could make arrangements with the electric power provider to have power routed to the base by another substation. Three, the Marines, in conjunction with the electric power provider and local civilian authorities, could harden the facility by moving the fence line out further to lessen the effects of a blast, also making it much more difficult for unauthorized vehicles to be able to circumvent the "pole" barrier. Four, the Marines could make arrangements with the power provider to establish redundant means of providing electric power to the base, thus lessening the impact of the destruction of any one substation. Finally, another alternative would be to have established a pre-arranged agreement with civilian guard forces to be deployed during a time of heightened security to ensure the integrity of the power station.

4.3 Computer Network Defense Vulnerability Remediation

With computer systems taking such a preeminent role in today's society, Computer Network Defense (CND) has become extremely important. Computers are involved in almost every aspect of our lives, and any disruption of that system will adversely affect the way we do business. In fact, information technology (IT) has become so important to military operations that disruption of that service could even affect the outcome of a war.

Our computer systems and associated equipment must be protected from any and all intrusions by people with criminal intent. One of the best methods to do this is to assess a Navy or Marine Corps installation's computer system to determine if it has any vulnerabilities. Once these vulnerabilities are identified, they can then be prioritized according to their relative importance to the Installation Owner/Base Commander. At that point, these vulnerabilities should be remediated to ensure that the IT network is protected from any internal or external attack.

To assist Installation Owners/Base Commanders in their remediation efforts, the following examples of CND vulnerabilities and remediation are provided.



■ Computer Network Defense Vulnerability: NETWORK PROCEDURES

Vulnerability: During a recent NIVA of a Naval Installation, representatives of the Fleet Information Warfare Center (FIWC) discovered very lax password procedures by both military and civilian employees. Some employees had their passwords written on paper stuck to their computer monitors or keyboards, and many employees had not used the proper character, number or special characters for their passwords. This lack of adherence to proper network procedures made the entire system susceptible to attack by potentially allowing unauthorized persons access to the network.

Remediation: In this case, the Command should enforce a strong password policy concerning periodic change requirements. This password policy should include forbidding employees from exchanging passwords or writing their passwords anywhere. Further, they should require employees to use the minimum character set (eight characters) including at least

one special character and one numeral in all of their passwords. All of these remediation efforts must be enforced by the management to ensure compliance by all employees. This approach holds whether the network is a legacy network or has come under the NMCI umbrella. NMCI will apply a periodic forced password change protocol but legacy networks would be well advised to employ a periodic password change policy if one does not already exist.

■ Computer Network Defense Vulnerability: **HARDWARE/SOFTWARE**

Vulnerability: In a NIVA onboard a Naval facility that has come under the operational control of NMCI, the following vulnerabilities were discovered associated with their computer network: missing firewall protection; no virus scanning software; incorrect configuration of routers and ports; unprotected "dial-up" access to networks; un-patched software; and, lack of compliance with the DoD Information Assurance Vulnerability Alert (IAVA) Program. All of these hardware and software vulnerabilities left their network very susceptible to penetration.

Remediation: To remediate these vulnerabilities, the asset owner (the NMCI contractor) exercises operational control and responsibility for the network. The Base/Installation Commander, however, has a vested interest in ensuring that networks are accessible for Navy/Marine Corps personnel. In addressing possible remediation, the Base/Installation Commander would want to include the OIC, CNNOSC Detachment from the regional NOC to get periodic update/status reports on remediation actions being taken by the contractor to ensure the integrity of the Base/installation networks and to eliminate or reduce the vulnerability exposure posed by non-compliance with existing IAVA guidance. In this case, installation of a firewall; installing and maintaining updated Virus Scanning Software on all desktop computers; closing all unnecessary router/device ports; segregating or eliminating external modem "dial-up" capability from the rest of the network; as well as full compliance with existing IAVA direction will effectively address the vulnerabilities described in this example. The NMCI administrator can assist in brainstorming other remediation methods.

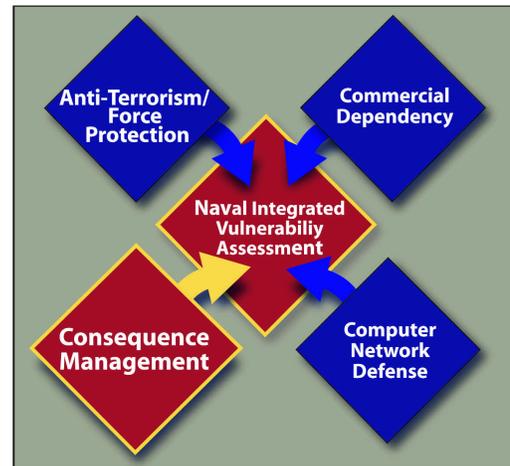
■ Computer Network Defense Vulnerability: **SECURITY AWARENESS**

Vulnerability: A NIVA of another Naval facility disclosed that no formal or periodic Information Security (IS) or Information Assurance (IA) awareness program was in effect for the organization. Further, there was a lack of minimum knowledge and skills evaluation to ensure that everyone involved in the use of computer/network resources was qualified to do their job. This vulnerability could result in a serious compromise of the network due to a lax security posture and the poor qualifications of command personnel.

Remediation: In this case, under legacy network operation or NMCI, the following remediation measures could be implemented to resolve these vulnerabilities: implement IS/IA awareness training for all personnel; and, require at least an annual test of knowledge and awareness of policies and procedures. This approach would provide the necessary training and awareness program to ensure that all employees were aware of IS/IA policies.

4.4 Consequence Management Vulnerability Remediation

An Installation Commander's Consequence Management (CM) program consists of four components: the Response Plan; the Continuity of Operations Plan (COOP Plan); the Recovery Plan; and the Reconstitution Plan. The dominant plan of these four is the COOP Plan, which focuses on maintaining the operation of Mission Essential Functions (MEFs) in support of critical assets without interruption or degradation of service. The Response Plan is primarily focused on the immediate reaction and response to a disaster whether natural, accidental, or a terrorist attack. The Recovery Plan concerns itself with the recovery and restoration of the operational capabilities of MEFs in support of critical assets. Lastly, the Reconstitution Plan contains the long-term requirements to either restore the critical asset to its original pre-disaster event design and function, or incorporate new technology, processes, construction techniques, etc., to improve functionality and survivability.



Additional information about CM and the DON can be found in the Department of the Navy (DON) Critical Infrastructure Protection (CIP) CM Planning Guide. One of the most important points to remember about CM is that the planning occurs long before a disruptive event, but the actual execution of the CM plan occurs after the disruptive event. Figure 4-1 depicts this timing relationship between planning and executing a CM plan.

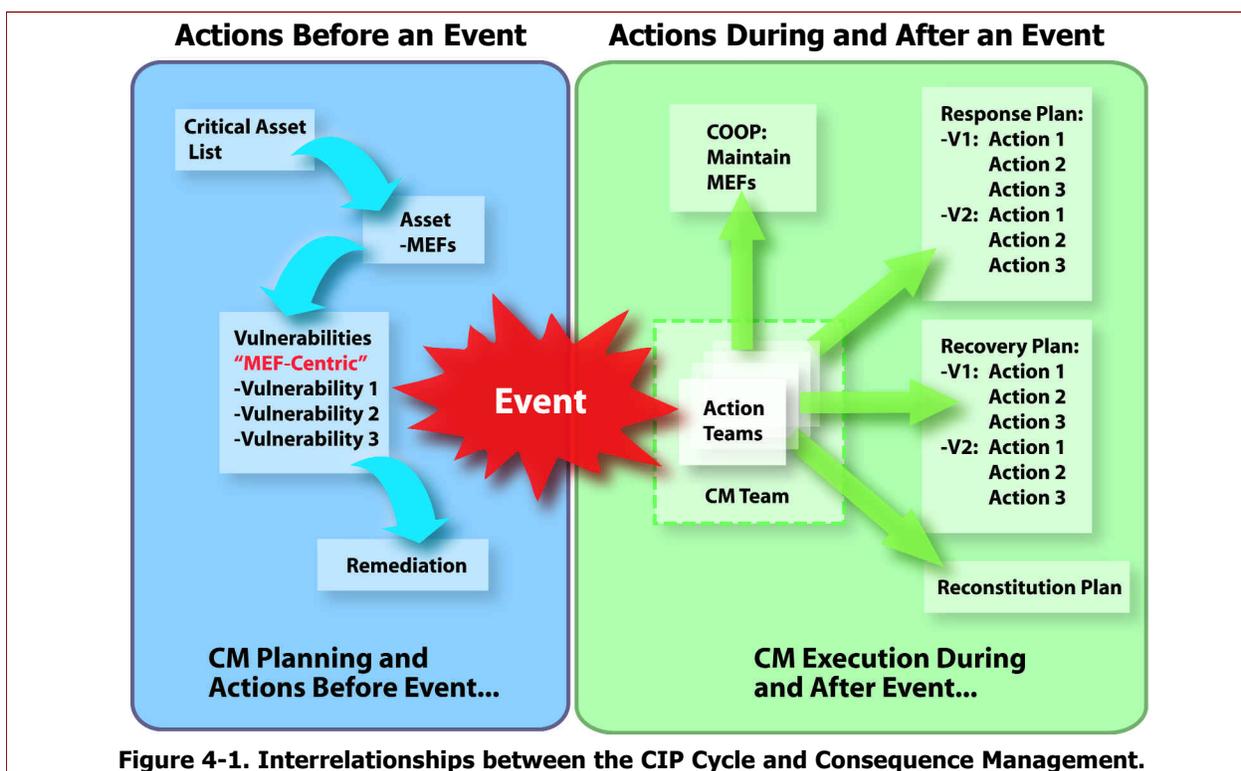


Figure 4-1. Interrelationships between the CIP Cycle and Consequence Management.

This Remediation Guide focuses on the CM planning done prior to any disaster event. It is during this CM planning that certain vulnerabilities are likely to be discovered that might not otherwise be noticed. While NIVAs are most likely to find vulnerabilities in physical security, cyber, and commercial dependency assets, only the CM planning phase can find vulnerabilities associated with COOP, response, recovery and reconstitution.

It is the vulnerabilities discovered during CM planning that are the focus here, as well as what priority these vulnerabilities might receive over vulnerabilities found during the other three NIVA pillars. Examples of CM related vulnerabilities and their remediation are provided below.

■ **CM Planning Vulnerability: NO CORPORATE MEMORY REDUNDANCY**

Vulnerability: During a NIVA of a highly sensitive intelligence and telecommunications site, the CM team noticed that several employees in a particular area of this site had all been doing the same jobs for almost 40 years. In fact, because of their lengthy service, they were the corporate history for this area, and the facility had no back-up or anyone else who could do these very sensitive functions. The loss or incapacitation of these individuals would literally mean loss of this function. This proved to be a single point of failure for this intelligence and telecommunications site.

Remediation: In this case, there are fewer options than in some of the other examples. Perhaps the best method of remediating this vulnerability would be to begin inserting less experienced employees into this area to work with more experienced employees, so that a smooth transition can be made. Another option might be to have the current employees codify their procedures and work requirements into a written document so that it can be used for training others in the event all of these employees were lost due to a disaster. It is also possible that future technology might override the need to fill these current positions, but that might not be a short-term solution. Initially, the continuity of operations would have to be accomplished by personnel trained in the specialties of the experienced employees.

■ **CM Planning Vulnerability: ACCESS FOR FIRST RESPONDERS**

Vulnerability: During a recent NIVA, the CM team noted that in the response plan of a Naval Base the first responders would not be able to access certain parts of the base because of the tight security instituted as a result of a disaster event. The planned security measures were appropriate for the nature of the event, but did not consider the necessity to permit first responders to pass through the security barrier in order to fight fires and care for casualties. The assessment also pointed out how "stove piped" plans can result when all stake holders are not involved in the process.

Remediation: The CM Plan should be rewritten to include procedures allowing first responders to access the necessary parts of the Naval Base in the event of an emergency. While security should remain tight aboard the Naval facility, it should not interfere with the emergency personnel trying to do their job. This should be a well-coordinated effort between first responders and security.

■ **CM Planning Vulnerability: BACKUP PLAN FOR SOFTWARE**

Vulnerability: The Operations Department aboard an installation identified its critical computer systems to the Information Technology (IT) Department for recovery during an event. These legacy systems provide critical command and control systems necessary to maintain base

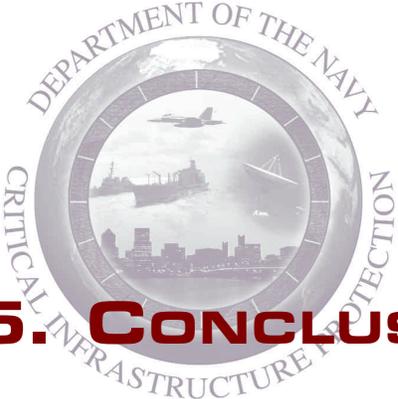
functions. They run on servers co-located within the Operations Department. A review of the IT Department Recovery Plans outlined how they would recover the network, servers, and data. However, the plans did not address the procedures to identify, obtain, and store application software separate from the office that used it. As a result, the IT Department was unaware of the software applications necessary to recover the systems. Since many offices maintained the only copy of the software applications, if a particular office were lost during an event such as a fire, the IT Department would have been unable to reload the application software in a timely manner. This would have delayed the recovery of the Operations Department's ability to perform its mission essential functions.

Remediation: Users must identify to the IT Department all critical systems necessary to sustain base operations. The IT recovery plan needs to integrate all primary and secondary actions (internal and external) necessary to recover each system. Back-up data, applications, and hardware equipment needed to recover a particular system must not be co-located in the same facility as the original system.

This page left blank intentionally.



Conclusion



5. CONCLUSION

The purpose of remediation is to reduce or eliminate vulnerability and any resulting capacity to disable a mission critical function/asset. Remediation strategies should be developed to provide the most protection while balancing resources and risk. In some situations, a useful strategy may be to achieve graceful degradation in systems and assets, should an attack or other disruptive event occur.

Within the CIP Event Cycle, remediation bridges the gap between the analysis and assessment phase and the consequence management sequence of phases by improving the reliability, availability, and survivability of critical assets and/or infrastructure. In most cases, the cost of remediation (in terms of manpower, money, and time) is almost always less than the cost of managing the consequences of a successful assault involving an unremediated vulnerability.

In most cases, the cost of remediation (in terms of manpower, money, and time) is almost always less than the cost of managing the consequences of a successful assault involving an unremediated vulnerability.

Achieving positive results requires a holistic approach, integrating the contributions of several focus areas into a single plan that addresses all characteristics of the vulnerability being remediated. There is no one set of answers; each case must be assessed and approached based on its own set of variables. Instead of attempting to provide all possible solutions, this guide provides a framework from which those involved in remediation can develop a specific approach and plan of action that meets their own specific needs and requirements.

For additional information and/or guidance from the DON CIAO staff on vulnerability remediation, please contact those listed below.

■ **Points of Contact:**

- ◆ DON CIAO Team Leader - 703.602.4412
- ◆ DON CIAO Staff - 703.601.1214 or 703.602.6759

This page left blank intentionally.



Appendices

Appendix A: Terminology

Appendix B: Acronyms

Appendix C: Remediation Timeline

APPENDIX A - TERMINOLOGY

ASSESSMENT (CIP): (1) An assessment is an objective evaluation of the vulnerabilities associated with Joint Force Capabilities. (2) Objective determination of how critical the capability and supporting infrastructure is in supporting military operations that accomplish the National Military Strategy. Focus is Combatant Command OPLANs. (3) A process to characterize DoD infrastructure, their dependencies and interdependencies and subsequent linkages to commercial, foreign and host nation infrastructure.

ASSET: Any military/private/commercial resource, relationship, instrument, installation, supply or system that in some combination is used in a military operational or support role. Assets are found at CONUS and OCONUS locations.

ASSET CRITICALITY: Measure of impact of asset that supports other assets, infrastructure, or operational plans.

CAPABILITY (Regional Combatant Commander/Joint Force): MILITARY CAPABILITY: The ability to achieve a specific wartime objective (win a war or battle, destroy a target set). It includes four major components: force structure, modernization, readiness, and sustainability. (a) Force structure - Numbers, size, and composition of the units that comprise our Defense forces; e.g., divisions, ships, airwings. (b) Modernization - Technical sophistication of forces, units weapons systems, and equipment. (c) Unit Readiness - The ability to provide capabilities required by the Combatant Commanders to execute their assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed. (d) Sustainability - The ability to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, materials, and consumables necessary to support military effort.

CRITICAL ASSET: (1) Asset that can be either a DoD or non-DoD military-related unit, organization, facility, installation, system, resource, equipment, instrument, which is identified as performing an *essential* service, function, or use in military operational plans or support to operational plans. (2) Any facility, equipment, service or resource considered *essential* to DoD operations in peace, crisis and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and timely restoration. Critical Assets may also be DoD assets or other government or private assets, domestic or foreign, whose disruption or loss would render other DoD Critical Assets ineffective or otherwise seriously disrupt DoD operations. Critical Assets include both traditional "physical" facilities and equipment, non-physical assets (such as software systems) or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).

CRITICAL INFRASTRUCTURE: Those systems and assets (both government and private) essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department of Defense to execute the National Military Strategy.

CRITICAL INFRASTRUCTURE ASSURANCE OFFICER (CIAO): The CIAO is responsible for the protection of all of the Department's critical infrastructure to assure that they can support the mission of the organization. The CIAO has established procedures for obtaining expedient and valid authority to allow vulnerability assessments to be performed on physical assets and computer/cyber systems. The Department of the Navy CIAO is the Department of the Navy Chief Information Officer, who was initially appointed by Under Secretary of the Navy Memorandum of 26 August 1999. In addition to other duties concerning DON physical and cyber protection and readiness, the DON CIAO chairs the DON Critical Infrastructure Protection Council.

CRITICAL INFRASTRUCTURE PROTECTION: CIP is Mission Protection. CIP is the identification, assessment, and assurance of Cyber and Physical infrastructure that support mission critical capabilities and requirements, to include the political, economic, technological, and informational security environments essential to the execution of the National Military Strategy.

CRITICAL INFRASTRUCTURE PROTECTION COUNCIL: The DON Critical Infrastructure Protection Council: (a) determines the necessary efforts to institute Critical Infrastructure Protection throughout the DON; (b) contributes subject matter experts to support OSD sector CIAOs; (c) identifies resource sponsors and asset owners responsible for DON critical infrastructure; and recommends resource actions to support implementation.

DoD INSTALLATION: A facility subject to the custody, jurisdiction, or administration of any DoD Component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, or laboratories where a DoD Component has operational responsibility for facility security and defense. Examples are facilities where the military commander or other specified DoD official under provisions of DoD Directive 5200.8, 25 April 1991, has issued orders or regulations for protection and security. Both industrial assets and infrastructure assets, not owned by the Department of Defense, may exist within the boundaries of a military installation

FORCE PROTECTION: Security program designed to protect Service members, civilian employees, family members, facilities and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE - 7 (HSPD-7): This December 2003 directive on Critical Infrastructure Identification, Prioritization and Protection establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. It states that Federal departments (DoD) and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them; and that Federal departments and agencies will work with State and Local governments and the private sector to accomplish this objective. It further states

that all Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms: (a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and (b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. This directive supersedes Presidential Decision Directive/NSC-63 of May 22, 1998 ("Critical Infrastructure Protection"), and any Presidential directives issued prior to this directive to the extent of any inconsistency.

IMPACT ANALYSIS: The process of identifying an organization's exposure to the sudden loss of selected business functions and/or the supporting resources (threats), and analyzing the potential disruptive impact of those exposures (risks) on key business functions and critical business operations.

INDICATIONS AND WARNING: Indications are preparatory actions or preliminary infrastructure states that signify that an incident is likely, planned, or is underway. An official warning would be issued by the responsible organization.

INFORMATION ASSURANCE (IA): (1) Information Operations 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 incorporating protection, detection, and reaction capabilities. (2) Information operations that protect key public and private elements of the national information infrastructure from exploitation, degradation, and denial of service.

INFORMATION SECURITY: Information Security is the protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information Security includes these measures necessary to detect, document, and counter such threats. Information Security is composed of computer security and communications security. Also called INFOSEC.

INFORMATION SYSTEM: The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information.

INFRASTRUCTURE: The framework of inter-dependent networks and systems comprising identifiable industries, institutions, functions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole.

INFRASTRUCTURE ASSET: Any infrastructure facility, equipment, service or resource that supports a DoD Component. A Critical Infrastructure Asset is an infrastructure asset deemed essential to DoD operations or the functioning of a Critical Asset.

INFRASTRUCTURE ASSURANCE: Planning to improve the readiness, reliability, and continuity of infrastructure such that they are: (1) less vulnerable to disruptions or attack; (2) harmed to a lesser degree in event of disruption or attack; and (3) can be readily reconstituted to reestablish vital

capabilities. It includes those efforts that protect infrastructure, assure their readiness, reliability, and continuity of infrastructure such that they are: less vulnerable to disruptions or attack, harmed to a lesser degree in the event of a disruption or attack, and can be readily reconstituted to reestablish vital capabilities. (DoD CIP Plan) Preparatory and reactive risk management actions intended to increase confidence that a critical infrastructure's performance level will continue to meet customer expectations despite incurring threat inflicted damage, e.g., incident mitigation, incident response, and service restoration.

INFRASTRUCTURE INDICATIONS & WARNING: Tactical indications through the implementation of sector monitoring and reporting, strategic indications through Intelligence Community support, and warning in coordination with the National Infrastructure Protection Center (NIPC) in concert with existing DoD and national capabilities.

INFRASTRUCTURE PROTECTION: Proactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructure. For instance, threat deterrence and vulnerability defense.

INTERDEPENDENCE: Dependence among elements or sites of different infrastructure, and therefore, effects of one infrastructure upon another.

MISSION CRITICAL: Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness and must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information).

MISSION ESSENTIAL: Any asset or function that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

MITIGATION: Action taken to reduce or eliminate vulnerability of people or infrastructure to threats and their effects.

NAVAL INTEGRATED VULNERABILITY ASSESSMENT: An expert third party or peer review comprehensive CIP assessment instrument under DON CIAO coordination and leadership synthesizing several existing assessment protocols including Marine Corps or CNO Integrated Vulnerability Assessments for Anti-terrorism and Force Protection; Marine Corps Network Operations and Security Command (MCNOSC) or Fleet Information Warfare Center (FIWC) assessments for computer network vulnerability; non-organic and other commercial infrastructure assessments performed by DPO-MA (formerly Joint Program Office - Special Technology Countermeasures (JPO-STC)) or other; and a continuity of operations plans and preparedness assessment under appropriate Navy or Marine Corps community direction. The NIVA is performed cyclically in all Navy Regions or other major Navy concentration areas, and at major Marine Corps Installations.

NETWORK: Information system implemented with a collection of interconnected nodes.

OPERATIONAL IMPACT: Impact of critical assets and OPLANS on other military operations (mobilization, deployment, force projections, etc.).

OPERATIONAL IMPACT ANALYSIS: The relationship between military plans and operations and critical assets established through the development of operational dependency matrices and application of operations research methodologies.

PHYSICAL SECURITY: (1) 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. See also Communications Security, Protective Security, Security. (JP 1-02, p.343) (2) Actions taken for the purpose of restricting and limiting unauthorized access, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks, e.g., through the use of conventional or unconventional weapons.

RECONSTITUTION: Refers to actions required to rebuild or restore an aspect or portion of an infrastructure after it has been degraded. Owner/operator directed restoration of critical assets and/or infrastructure.

RECOVERY: Those long-term activities and programs which are designed to be implemented beyond the initial crisis period of an emergency or disaster in order to return all systems to normal status or to reconstitute those systems to a new condition that is less vulnerable.

RELIABILITY: The capability of a computer, or information or telecommunications system to perform consistently and precisely, according to its specifications and design requirements, and to do so with high confidence.

REMEDIATION: Those precautionary actions taken before undesirable events occur to improve known deficiencies and weaknesses that could cause an outage or compromise a defense infrastructure sector or critical asset. Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc., of critical assets and/or infrastructure, e.g., emergency planning for load shedding, graceful degradation, and priority restoration; increased awareness, training, and education; changes in business practices or operating procedures, asset hardening or design improvements, and system-level changes such as physical diversity, deception, redundancy, and back-ups. Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc. of critical assets and/or infrastructure, e.g., emergency planning for load shedding, graceful degradation and priority restoration; increased awareness, training and education; changes in business practices or operating procedures, asset hardening or design improvements, and system level changes such as physical diversity, deception, redundancy and backups.

RESPONSE: Response refers to those activities undertaken to eliminate the cause or source of an event. It also includes emergency measures from dedicated third parties such as medical, police, and fire and rescue (Public Safety). Coordinated third party (not owner/operator) emergency (e.g., medical, fire, hazardous or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident.

RESTORATION: The act of returning a piece of equipment or some other resource to operational status. Commercial service companies provide a restoration service with staff skilled in restoring sensitive equipment or large facilities. Such vendors often work with insurance companies and may restore equipment for a fee or may purchase damaged equipment with the intent of restoring the equipment and re-marketing the product.

RISK: The probability that a particular threat will exploit a particular vulnerability of the system. The probability that a particular critical infrastructure's vulnerability being exploited by a particular threat weighted by the impact of that exploitation.

RISK ANALYSIS OR RISK ASSESSMENT: The process of identifying security risks, determining their magnitudes, and identifying areas needing safeguards. Risk Analysis is part of Risk Management produced from the combination of Threat and Vulnerability Assessments characterized by analyzing the probability of destruction or incapacitation resulting from a threat's exploitation of a critical infrastructure's vulnerabilities.

RISK MANAGEMENT: The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review (NSA, NCSC Glossary, Oct 88.) The deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, characterized by identifying, measuring and controlling risks to a level commensurate with an assigned value.

THREAT: A foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and malicious intent of debilitating the defense or economic security of the United States. A threat may be an individual, organization, or nation.

THREAT ANALYSIS: A continual process of compiling and examining all available information concerning potential conventional and asymmetric force activities by groups which would target a asset, facility, node, capability, or infrastructure. A threat analysis will review the factors of a hostile groups' existence, capability, intentions, history and targeting as well as the security environment within which the friendly forces operate. Threat analysis is an essential step in identifying probability of conventional/ asymmetric attacks and results in a threat assessment.

TIER DEFINITIONS: As determined by the Regional Combatant Commanders:

- Tier I - Warfighter suffers strategic mission failure. Specific timeframes and scenarios assist in infrastructure prioritization.
- Tier II - Sector or element suffers strategic functional failure, but Warfighter strategic mission is accomplished.
- Tier III - Individual element failures, but no debilitating strategic mission or core function impacts occur.
- Tier IV - Everything else.

VITAL RECORDS: Records or documents, regardless of media (paper, microfilm, audio or video tape, computer disks, etc.) which, if damaged or destroyed, would disrupt business operations and information flows and cause considerable inconvenience and require replacement or recreation at considerable expense.

VULNERABILITY: (1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (2) The characteristics of a system which cause it to suffer a definite degradation (incapacity to perform the designated mission) as a result of having been subjected to a certain level of effects in a unnatural (manmade) hostile environment. (3) In information operations, a weakness in infor-

mation system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. A characteristic of a critical infrastructure design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat.

VULNERABILITY ASSESSMENT: Assessment of probability that events will occur using scenario-driven vulnerability index. Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.

This page left blank intentionally.

APPENDIX B - ACRONYMS

-A-

AOR	Area of Responsibility
AOR	Assumption of Responsibility
AT/FP	Anti-Terrorism/Force Protection

-C-

CD	Commercial Dependency
CIAO	Critical Infrastructure Assurance Officer
CIP	Critical Infrastructure Protection
CIO	Chief Information Officer
CM	Consequence Management
CND	Computer Network Defense
CNI	Commander, Naval Installations
CO	Contracting Officer
COOP	Continuity of Operations Plan

-D-

DoD	Department of Defense
DON	Department of the Navy
DPO-MA	Defense Program Office - Mission Assurance

-E-

AFP	Engineering Field Personnel
-----	-----------------------------

-F-

FIWC	Fleet Information Warfare Center
------	----------------------------------

-H-

HSPD-7	Homeland Security Presidential Directive - 7
--------	--

-I-

IA	Information Assurance
IAVAP	Information Assurance Vulnerability Alert Program (DoD)
IS	Information Security
ISSO	Information Systems Security Officer
IT	Information Technology

-M-

MCNOSC	Marine Corps Network Operations & Security Command
MEF	Mission Essential Functions
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding

-N-

NAVFAC	Naval Facilities Engineering Command
NIVA	Naval Integrated Vulnerability Assessment
NMCI	Navy and Marine Corps Intranet
NOC	Network Operations Center

-O-

OPLAN	Operational Plan
-------	------------------

-P-

POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
PDD-63	Presidential Decision Directive 63
PWO	Public Works Officer

-V-

VA	Vulnerability Assessment
----	--------------------------

APPENDIX C - REMEDIATION TIMELINE

General Remediation Process Timeline & Checklist

- 1. Receive Initial Vulnerability Information** via DON NIVA outbrief or as generated through the use of the DON CIP Self Assessment Tool & Reference Guide
- 2. Establish a Command Point of Contact and/or Action Officer**
- 3. Determine and Designate a Command Remediation Team (CRT):** Composition based on types and areas of vulnerability to be addressed, e.g.:
 - Commander, Naval Installations (CNI) Staff
 - Contracting Officer
 - Critical Infrastructure Protection (CIP) or AT/FP Officer
 - Engineering Field Personnel (EFP)
 - Information Systems Security Officer (ISSO)
 - Officer-In-Charge, Commander Naval Networks and Space Operations Command (OIC CNNSOC)
 - Public Works Officer (PWO)/Staff Civil Engineer
 - Regional Commander's Staff
 - Security Officer
 - Others as may be required
- 4. As Necessary, Establish a Baseline of Training and Information in:**
 - Critical Infrastructure Protection
 - Mission Essential Functions
 - Naval Integrated Vulnerability Assessments
 - Vulnerability Remediation
 - The vulnerabilities identified
- 5. As Soon as Possible After Single Points of Failure are Identified:**
 - Review and prioritize vulnerabilities.
 - Confirm ownership of assets involved
- 6. Ideally, Within 30 days after Identifying Single Points of Failure:**
 - Evaluate options: balance risk vs cost vs mission assurance
 - Determine those options most logical, cost effective, and threat-impact effective
- 6. As Soon as Possible; NLT 60 Days of Assessment Report:**
 - CRT creates plans with timelines for accomplishing selected approach
 - Installation Owner/Base Commander seeks support for resources required to implement remediation through Chain of Command to include, as appropriate, Regional Combatant Commander; the Region; and Commander, Naval Installations (CNI)
- 7. W/in 2-4 Weeks of Plan Approval:**
 - Installation Owner/Base Commander implements Remediation Plan
 - Appropriate senior officials are notified that remediation has begun at Plan commencement
- 8. W/in 15 Days of Vulnerability Remediation/Plan Completion:**
 - All appropriate senior officials are notified
- 9. One Year after Receipt of Assessment Report, as Applicable:**
 - If effort is long term, a follow-up report re: status and estimate of completion is provided to senior officials/appropriate chain of command
- 10. Three Years after Assessment:** Next NIVA or self assessment is due

NOTE: Notification of senior officials, including the service lead for critical infrastructure protection, will allow data bases used for Indications & Warning (such as the DON CIP Data Management System at Naval Criminal Investigative Service (NCIS) Headquarters) to be kept updated/accurate concerning current Navy-wide vulnerabilities and their status.