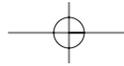


Critical Infrastructure Protection Campaign Plan



UNITED STATES MARINE CORPS





Introduction



“The recent terrorist attacks on our nation highlight the new reality of warfare. The very visible attacks against icons of our democratic nation and our citizens no longer represent a simple violation of international law. As was evidenced so graphically both in New York City and in Washington, a new form of open warfare was declared against America, directly targeting civilian and military personnel and our institutions alike...

As we respond to this tragedy, our focus, as always, is to mission first and people always...The very public display of this new form of warfare comes as no surprise to Marines. Our focus on developing Anti-Terrorism and Force Protection (AT/FP) capabilities across our forces continues our tradition of innovation and transformation...While our expeditionary culture remains the centerpiece of our Warfighting capability, the added ability to effectively deal with terrorism is critical today and will remain one of our core capabilities for the foreseeable future...

In order to continue our tradition of innovation we must capture the lessons we have learned regarding this emergent form of warfare.”

General James L. Jones
U.S. Marine Corps, Commandant
ALMAR 041/01, September 12, 2001.

The terrorist attacks of September 11th were, by no means, terrorists' first efforts to influence U.S. actions through violence. The Beirut barracks, Khobar Towers, the U.S. Embassies in Africa, and the Cole bombings are other recent examples, but the September 11th attacks prove the enemy has become bolder and that the U.S. is vulnerable within its borders. The Marine Corps shares these vulnerabilities, both at home and abroad.

While terrorist actions will never result in the defeat of the Marine Corps, successful terrorist actions could prevent the Marine Corps from fulfilling mission objectives as planned, and with today's military operations dependent on speed, flexibility and precision, a delay or disruption could have serious repercussions.

As Marines, our success is determined by our ability to rapidly task organize, deploy, and engage the enemy with superior skill, firepower, and logistic support. Clearly, protecting the infrastructure that enables our forces to be successful is of paramount importance. Assuring the availability of such mission essential assets is known as Critical Infrastructure Protection (CIP). As the Director of the Marine Corps CIP program, my objective is to assure that Marine Corps critical assets are available to support our missions, from peace keeping to the decisive engagement and defeat of our nation's foes.

Mission critical assets are vulnerable to a wide range of conventional and asymmetrical threats, including chemical, biological, radiological, cyber and nuclear. Our history of leading in the development of Anti-terrorism and Force Protection (AT/FP) measures will serve as the tactical building blocks in the strategic planning and implementation of a fully integrated CIP capability.



Scenario

Hostile forces in the Far East have invaded a long standing ally of the United States, precipitating a substantial U.S. military response to protect vital resources in the region. Taking advantage of this opportunity, a smaller rogue nation in the Middle East decides to invade a neighboring country in the hopes of securing a rapid victory and then suing for peace.

Being experienced war fighters, the importance of risk mitigation strategies and contingency planning is well understood. In CIP this means reducing vulnerabilities, and in the event of an attack, developing plans for restoration and recovery. Further, training for such events is essential. Being pragmatic, it is clear all CIP initiatives cannot be undertaken simultaneously. Therefore, we must continually assess our situation and prioritize our efforts, maximizing the effectiveness of the Marine Corps investment in CIP and assuring the Marine Corps has the CIP resources required to move forward.

Our missions will continue to be broad in scope and geography, and our interactions with other forces will increase in frequency and complexity. These relationships will continue to underscore the importance of the Marine Corps' ability to rapidly task organize, deploy and successfully carry out its missions. We must act with determination to identify, assess, and assure that our essential cyber and physical mission critical capabilities are protected and available for the execution of our missions. Within this enormous task, we must also plan beyond the military community, integrating crucial civilian and commercial infrastructures vital to mission success and

continuity of operations. We must also expand and incorporate our CIP knowledge and capabilities in core training, education and acquisition programs.



In doing so, we will not fail to deliver what our Nation expects of its Marines – winning battles and accomplishing their missions.

Emil R. Bedard
Lieutenant General
U.S. Marine Corps

To widen their window of opportunity, this rogue nation solicits the help of a terrorist organization, which results in the activation of several sleeper terrorists' cells in the United States whose objective is to delay and disrupt U.S. military force deployments. These terrorists cells, knowledgeable of U.S. military operations and power projection from open source material written after the 1991 Gulf War, target key elements of the deployment infrastructure. In rapid succession, the following events occur:

- An east coast AFB airborne heavy rigging facility is rendered inoperative by a crop duster disbursing a suspicious substance.
- An unknown email virus has been detected at an east coast military base, resulting in the shut down of the unclassified email system, the destruction of files, and the temporary inability to transmit tasking. The virus has the ability to spread to bases globally within a few hours.
- A key logistics base for loading amphibious ships is blocked when a fully loaded oil tanker is set ablaze and sinks in the channel.
- A west coast military base is isolated when the overpass connecting the base to the freeway system is destroyed.
- Military intranet traffic is diminished when fiber optic cables connecting the network operations centers are severed.

While these events do not yield a crippling blow and may not result in a single casualty, the time phased deployment of forces has been disrupted, and U.S. military forces may be delayed and their immediate effectiveness diminished, giving the opponent time to accomplish his limited objectives.

The events of September 11th have shown us to expect the unexpected, and as the war on terrorism progresses, our nation's leaders have warned that future attacks within the United States must be anticipated. The mission of the Marine Corps CIP program is to prevent the disruption of Marine Corps operations related to the denial of availability of mission critical infrastructure.



The Marine Corps Approach to CIP

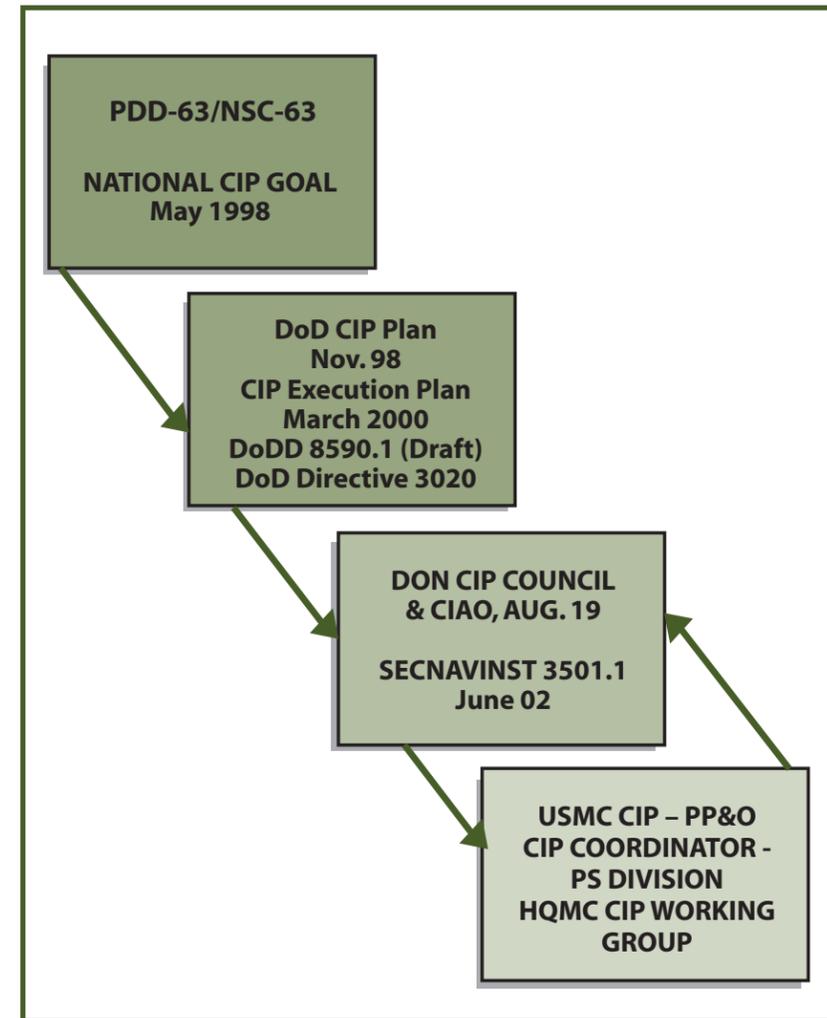
The Marine Corps views CIP and AT/FP as inextricably linked. CIP must be defined on both a strategic and tactical level. Our AT/FP capabilities will serve as tactical building blocks that support strategic CIP initiatives and program management. Fundamentally, CIP programs and initiatives will be planned and executed from an operational perspective, with one goal in mind—mission assurance. Both strategically and tactically the Marine Corps will forge a close working relationship with the Navy in developing an integrated CIP capability. This is a crucial task, as the Navy has been our enduring partner in littoral power projection, providing critical mission capabilities that support and sustain MAGTF expeditionary striking power.

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems...

As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

Presidential Decision Directive / NSC-63 (PDD-63)



GOAL: ENSURE THE COORDINATION AND DEVELOPMENT OF AN INTEGRATED CIP CAPABILITY



The U.S. Marine Corps and Critical Infrastructure Protection

What is Critical Infrastructure Protection?

“Critical Infrastructure Protection is Mission Protection. CIP is the identification, assessment, and assurance of cyber and physical infrastructures that support mission critical capabilities and requirements, to include the political, economic, technological and informational security environments essential to the execution of National Military Strategy.”

SECNAVINST 3501.1

Scope of Critical Infrastructure Protection.

Critical Infrastructure Protection involves a joint effort by not only the Marine Corps, but all DoD/DoN activities, federal and state civilian agencies, and our commercial partners, both at home and abroad. CIP requires all owners of infrastructure assets to understand the importance of their assets to War-fighter mission assurance, and to manage their dependencies and risk of loss or degradation.

Not every asset is critical to the accomplishment of a mission. Identifying and protecting assets that are critical to the accomplishment of the mission is the paramount goal of CIP. We must recognize that Marine Corps’ equipment, facilities, utilities, services, weapon systems, and mission accomplishment are highly dependent upon non-Marine Corps assets, including national/international infrastructures, facilities and services of the private sector, and other government departments and agencies. These non-Marine Corps assets are often essential to the execution of Marine Corps missions and their vulnerabilities are a cause for concern and require special attention.

Mission Critical Infrastructure

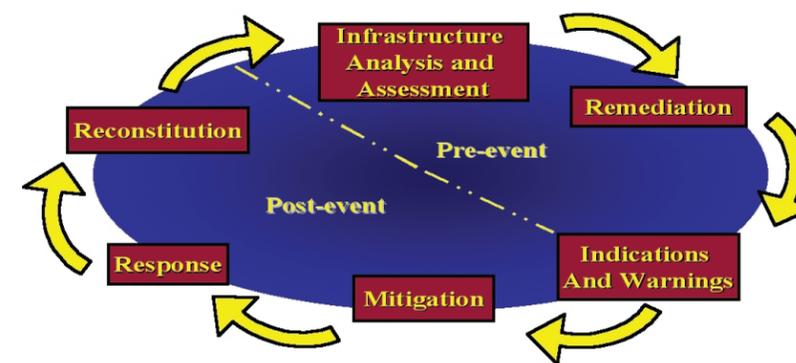
Infrastructure includes systems and assets that enable the Marine Corps to accomplish its war fighting mission, as well as its core business processes. Mission critical infrastructure are those assets and systems that are essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of DoD to execute National Military Strategy. (SECNAVINST 3501.1).

The CIP Process.

The effort to coordinate and integrate a CIP capability for the Marine Corps requires implementing a six-step assessment process, or event cycle, with respect to identifying and protecting our critical infrastructure. Those steps are: analysis & assessment; remediation; indications and warnings; mitigation; response; and reconstitution.

This six-step assessment process is fluid, and must be utilized on a continuing basis to ensure our Marines are capable of accomplishing their missions against a backdrop of changing threats and operating environments.

CIP EVENT CYCLE



In the following sections, important tasks and concepts associated with each step of the CIP process are discussed.

**Infrastructure Analysis and Assessment:
Identify Mission Critical Assets and Assess Their Vulnerabilities.**

Critical asset analysis and assessment is the foundation, and most important element, of the six CIP lifecycle events. To successfully defend against and respond to both conventional and asymmetric attacks upon our Nation, we must redefine the way we think about our mission critical assets. Each organization, installation, or unit must understand its mission and role in support of the Marine Corps Warfighting capability, and the essential assets that are contributed to support that Warfighting capability and ultimately, mission success. We must assure that these critical assets will be available when needed, and guard against their disruption or loss.



Tier Definitions of Critical Assets/Infrastructure:

Tier I - Assets whose loss or degradation could result in the Warfighter suffering strategic mission failure.

Tier II - Assets whose loss or degradation could result in a sector or element suffering a strategic functional failure, but the Warfighter strategic mission is accomplished.

Tier III - Assets whose loss or degradation could result in individual element failures, but no debilitating strategic mission or core function impacts occur.

Tier IV - Assets not included in Tiers I-III.

SECNAVINST 3501.1

We must focus on identifying and protecting our most critical assets first – assets which if lost or significantly disrupted would result in the Warfighter suffering a strategic mission failure. Once these assets are identified, a thorough analysis must be undertaken of the impact to mission assurance if any

such asset was lost or disrupted. Identification of all realistic threats and hazards, both conventional and asymmetrical, to each asset is crucial – and this is where we must change our mindset and modify traditional

CIP Identification and Vulnerability Assessment Tasks:

- **Confirm mission and role of organization/unit.**
- **Identify critical/key assets to be protected, and review the impact if those assets were lost. Review both USMC and privately owned assets.**
- **Value and prioritize assets based on consequences if they were lost.**
- **Conduct threat and hazard analysis. Identify threats, hazards (natural and man-made) and undesirable events to which each critical asset is exposed, and analyze the expected impact of each threat on each asset.**
- **Perform a vulnerability analysis and assessment of each critical asset to each specific threat and hazard.**
- **Develop a report containing individual and collective asset vulnerabilities.**

AT/FP doctrine. We must view our Homeland as part of the battlespace, and assess and revise our AT/FP, information security and operational security measures in this context.

For example, what are the single points of failure for privately owned critical assets the Marine Corps relies upon in telecommunications, electric power systems, fuel storage and transport, transportation, water supply systems, and emergency services? We must think critically about these assets, and undertake measures to assure that they are available when needed. The identification of our critical assets and the assessment of their vulnerabilities is crucial to our ultimate goal of achieving mission assurance.

GOAL: IDENTIFY CRITICAL ASSETS AND ASSESS THEIR VULNERABILITIES TO ALL THREATS.

Remediation.

Once critical assets and infrastructures have been identified by each installation or unit, and their vulnerabilities to a range of threats and hazards assessed, the immediate focus must then shift to identifying counter-measures that can be implemented before undesirable events or attacks occur. The goal is to eliminate known vulnerabilities, and improve the reliability and survivability of those assets.



Areas of Vulnerability.

- **In Antiterrorism (AT), a situation or circumstance, if left unchanged, that may result in the loss of life or damage to mission-critical resources.**
- **The characteristics of a system that 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 an unnatural (man-made) hostile environment.**
- **In information operations, a weakness in information security system 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.**
- **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 will to fight diminished.**

Remedial measures must be the result of integrating several factors, such as relative degree of risk to each asset, the likelihood that specific vulnerabilities will be exploited, and the cost-benefit of a range of proposed counter-measures. We

must engage in a comprehensive, service-wide risk management approach that looks at interdependencies and interoperability issues in developing and implementing the most appropriate counter-measures and remediation strategies.

Remediation Tasks:

- **Conduct an analytical risk assessment and determine the priorities for critical asset protection.**
- **Identify unacceptable risks and risk remediation priorities.**
- **Identify remediation and counter-measures recommendations, the costs, and conduct trade-offs in a cost-benefit analysis.**
- **Prioritize the counter-measure and remediation options that address identified risks.**
- **Obtain acceptance, direction and approval. Recommendations that are approved become the foundation of the CIP/AT/FP plan at the installation or base level.**
- **Prepare installation CIP/AT/FP plan as a single source document.**
- **Test, exercise and validate CIP/AT/FP plan.**
- **Develop and implement ongoing adjustments to CIP/AT/FP plan.**

Installations and units that may not be involved in a formal integrated vulnerability assessment program due to their small size may nonetheless house critical infrastructure assets that are vulnerable and in need of protective measures. CIP self-assessment tools and guidelines, as well as core training, education and awareness programs, shall be implemented and made available to all Marines.

GOAL: IDENTIFY AND IMPLEMENT PREVENTATIVE MEASURES THAT CAN BE UNDERTAKEN TO REDUCE RISKS OF LOSS, AND IMPROVE RELIABILITY AND SURVIVABILITY OF CRITICAL INFRASTRUCTURE ASSETS.



Indications and Warnings.

In the CIP event cycle, the initial focus was on “pre-event” activities. These activities required us to identify critical infrastructure assets and the spectrum of threats to those assets. We also analyzed each asset’s vulnerabilities to those threats, and identified and implemented appropriate remediation and counter-measure tactics and strategies.

Bridging the gap between pre-event preparation activities and post-event response activities is the Indications and Warnings phase of CIP. Vital to the protection of our critical infrastructure assets is the ability to deliver timely, accurate, and relevant intelligence to the field. We must coordinate collection, assessment, and dissemination of tactical and strategic indications and ensure rapid and timely transmission through a global, inter-agency rapid warning system.

We will work closely with the Navy, NCIS and the Director of Intelligence, HQMC, to establish a comprehensive and fully integrated I & W capability that will provide more accurate, timely, and relevant intel to our Marines worldwide.

Infrastructure Indications and Warnings Defined:

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.

Indications and Warnings Tasks:

- Establish a Marine Corps-Navy C2 system providing realtime, automated information, reporting and decision support to all echelons and for all levels of AT/FP.
- Coordinate I & W and Intel through NCIS, MTAC (Multiple Threat Alert Center) and ONI.
- Expand and integrate MTAC with NIPC, and other DoD and civilian CI organizations to produce real-time fusion and dissemination of I & W and Intel.
- Establish and integrate Force Protection Detachments in OCONUS locations devoid of permanent CI assets.
- Support establishment of daily tactical I & W product that fuses all relevant local, regional, and national force protection, intel and law enforcement data



GOAL: FULLY INTEGRATED AND COORDINATED TACTICAL AND STRATEGIC GLOBAL INDICATIONS AND WARNING CAPABILITY

Mitigation.

While our AT/FP efforts have always been focused on protecting the lives of Marines and their families, as well as the assets necessary to accomplish our mission, attacks upon our institutions and people in one form or another will undoubtedly occur in the future.



Our efforts to implement a CIP capability within the Marine Corps will not stop future attacks, whether by individuals, groups, or nations. CIP will make our people and assets less vulnerable, and help assure that mission critical assets will be available when needed.

Mitigation is a crucial component of CIP. Mitigation encompasses a range of preplanned and coordinated responses to infrastructure warnings and/or incidents. Actions in mitigation are generally undertaken by Marine Corps critical asset owners, installation commanders, resource sponsors and functional sector leads in responding to an infrastructure warning or incident.

CBRNE INSTALLATION EQUIPMENT PACKAGE

 RDR	 Portal Shield	 DFU
 ACADA		 PCR



Mitigation efforts do not prevent incidents, but are intended to reduce the impact or damage of the incident. Such efforts must involve the ability to detect attacks or threats, such as chemical, biological, and radiological, through the development and installation of state-of-the art CBRNE technology at critical Marine Corps sites.

Mitigation planning also requires that our First Responder communications equipment and mass notification systems be fully interoperable, intraoperable, and secure.

Mitigation Tasks:

- Support establishment and expansion of CBRNE preparedness and response programs.
- Develop and support fully interoperable capability for FirstResponder communications equipment and mass notification systems.
- Focus mitigation recommendations and efforts on reducing impact of single point failures of critical mission assets.
- Incorporate and integrate CIP mitigation planning in base or installation AT/FP plan.
- Develop mitigation plans to include Continuity of Operations (COOP) and Crisis Management planning.

MITIGATION GOALS: MINIMIZE ADVERSE EFFECTS ON A GIVEN MILITARY OPERATION OR INFRASTRUCTURE; FACILITATE RESPONSE TO THE WARNING OR INCIDENT; AND, RAPIDLY RESTORE THE INFRASTRUCTURE SERVICE DEGRADED BY THE INCIDENT.

Response.

In the context of the CIP life cycle the “response” stage occurs in the post-event or post-incident phase. An “attack” on our mission critical infrastructure or personnel, whether deliberate or the result of a natural disaster, has already occurred. Response will include those emergency activities that can assist Marine Corps personnel in eliminating the cause or source of an event.



Identifying and resolving significant planning, coordination, and interaction issues between the services, federal and state authorities in CONUS locations take on added urgency in the post-9/11 era. The Marine Corps will address, define and implement appropriate response measures, to include initial incident notification and situation reporting. Memoranda of

Response Defined:

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.

Response to infrastructure incidents involving Defense Infrastructure will follow one of two paths:

- (1) affected Components and/or the JTF-CNO (Computer Network Operations), will defend against and respond to all cyber incidents in accordance with granted authorities and established operational procedures, or
- (2) affected Components will defend against and respond to all non-cyber incidents in accordance with granted authorities and established operational procedures.



Understanding (MOU) and Memoranda of Agreement (MOA) with federal, state, and local governments need to be established, reviewed, and/or updated to address CIP response issues that the Marine Corps identifies in our vulnerability assessments.

Response Tasks:

- Coordinate Response requirements and protocols between the services.
- Identify Response requirements for sector business continuity planning.
- Construct coordinated Crisis/Consequence Management plan.
- Coordinate and integrate reporting mechanism requirements.
- Undertake installation assessment and modeling to help determine the best mix of Response equipment and location.
- Develop and implement CIP-specific post-incident assessments.

GOAL: SUPPORT THE DEVELOPMENT OF INCIDENT RESPONSE PLANS THAT WILL SUPPORT THE RAPID ELIMINATION OF THE CAUSE OR SOURCE OF AN INCIDENT, AND MINIMIZE ITS IMPACT.

Reconstitution.

The final stage of the CIP event cycle is Reconstitution. This is the process undertaken by the owner/operator of a critical infrastructure or asset which has been degraded or lost, to rebuild or restore that infrastructure or asset to operational capability.

Restoration of mission critical assets must involve close coordination between HQMC, PS Division, Critical Infrastructure Assurance Branch (PSC), resource sponsors and the operational chain of command. This coordinated effort will help ensure that the appropriate reconstitution measures are developed, implemented and integrated into Marine Corps operations and procurement planning efforts.

HQMC, PS Division, Critical Infrastructure Assurance Branch, (PSC), will facilitate the establishment of reconstitution plans, while ensuring that continuity of operations specifics are considered in such planning efforts. The HQMC CIP Working Group will also support DoN/DoD reconstitution efforts and organizations during crisis management.



Reconstitution Tasks:

- Identify Reconstitution requirements for continuity of operations.
- Facilitate in the establishment of Reconstitution plans, coordinating the requirements of resource sponsors and the operational chain of command.
- Support DoN/DoD Reconstitution efforts and organizations during crisis management.
- Incorporate CIP concepts and requirements within the acquisition process during Reconstitution.
- Prepare CIP-specific Reconstitution After-Action Assessments.

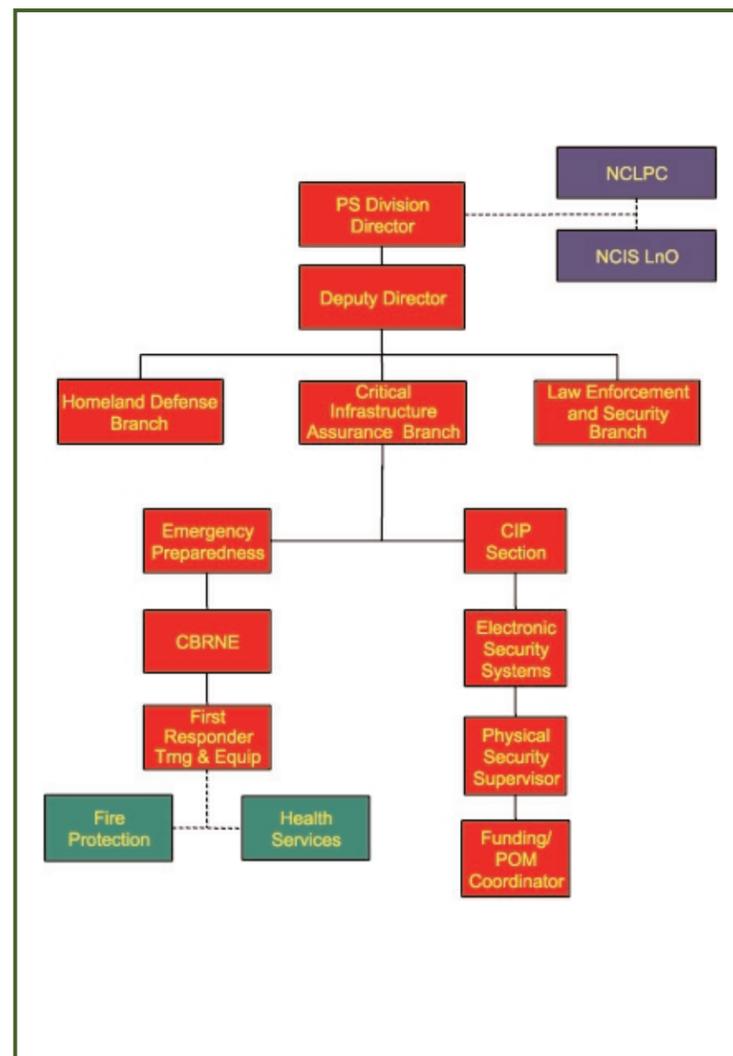
The Reconstitution stage also presents the immediate opportunity to ingrain CIP concepts and requirements in the acquisition planning and procurement process. While incorporating CIP requirements in the acquisition process is a fundamental, service-wide, long-term goal, we must be prepared to implement those requirements when restoring assets lost or degraded in an unplanned, immediate impact event.

We must develop a capability to fuse and integrate CIP concepts with the procurement acquisition process in a way that can be applied and implemented in emergent and critical situations requiring rapid response.

GOAL: TO REBUILD OR RESTORE MISSION CRITICAL INFRASTRUCTURE OR ASSETS THAT HAVE BEEN LOST OR DEGRADED TO FULL OPERATIONAL CAPACITY.



Critical Infrastructure Protection: USMC Organization and Task Flow

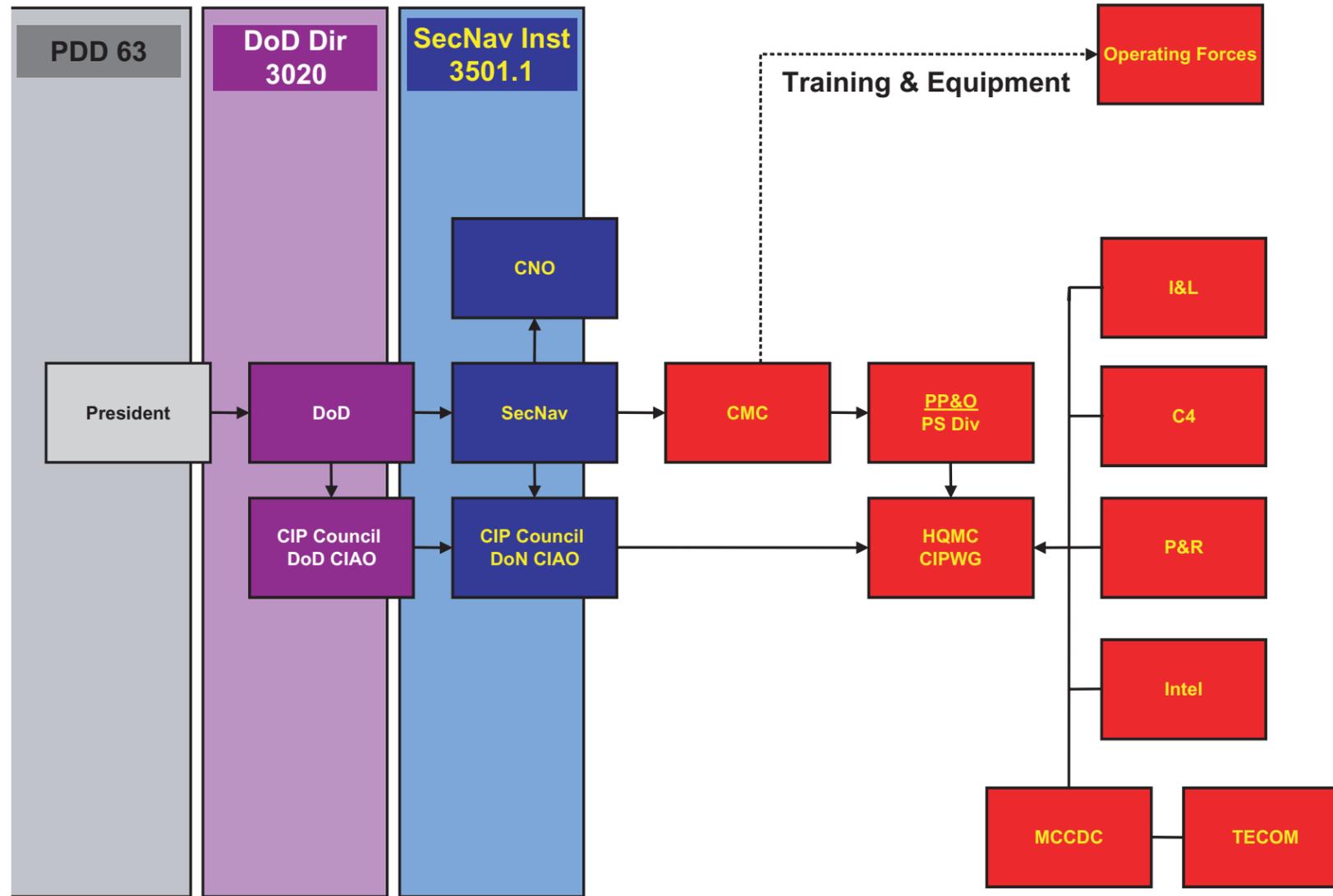


Authority of the Marine Corps to develop CIP policy and programs is based on a series of key Directives and Instructions, emanating from the Office of the President, down through the DoD to the Navy. Direct guidance for the Marine Corps flows from SECNAVINST 3501. In addition, the DOD and SECNAV CIP Councils provide high-level guidance for USMC coordination of CIP policies and programs.

The USMC coordinates its CIP policy through the Security Division, Critical Infrastructure Assurance (PSC) Branch, which drafts orders, regulations, and guidance in conjunction with the HQMC CIP Working Group. The Security Division falls under the authority of the Deputy Commandant for Plans, Policies, and Operations (DC, PP&O) who leads the development of CIP policy for the USMC. PP&O serves as the focal point for interface between the Marine Corps and the joint and combined activities of the JCS, the unified commands, and allied defense agencies. In addition, PP&O is responsible for developing and executing USMC plans and policies related to structure, deployment, and employment of forces.

The Deputy Commandant, PP&O, has delegated his responsibility for CIP development to the Security Division, which coordinates physical security plans, orders, policies, programs, and operational concepts. The Security Division serves as the single point of contact for internal and external coordination, development, articulation, and execution of Marine Corps CIP policies. The Security Division works in coordination with the branches that support it, including the Homeland Defense Branch, Security and Law Enforcement Branch, and the Critical Infrastructure Assurance Branch. There are several offices within each support branch that have specifically related CIP roles and responsibilities.

In addition, all HQMC organizations provide support to the Security Division in CIP policy and program development, and are active participants in the HQMC CIP Working Group.



KEY ORGANIZATIONS THAT SUPPORT USMC CIP POLICY AND PROGRAM DEVELOPMENT



The CIP Way Ahead – Mission First, People Always

The Marine Corps will aggressively move forward to accomplish its objectives in the vital area of Critical Infrastructure Protection (CIP). The objectives are to ensure that we protect assets and infrastructures deemed critical to Marine Corps operations in peace, crisis, and war; to mitigate the effect of their loss or disruption; and to plan for their timely restoration or recovery in the event of loss or degradation.

To meet these objectives, our initiatives shall include the following actions:

Policy and Guidance.

- Develop a baseline analysis of each USMC organization's roles, responsibilities, functions, and tasks directly related to planning and implementing CIP tasks and capabilities; and provide for periodic update.
- Establish clear lines of responsibility for *shared* mission critical assets between organizations with respect to CIP.
- Establish comprehensive resources and tools accessible to command to facilitate coordinated implementation of CIP tasks and capabilities.

Manpower Requirements.

- Identify and seek required personnel structure and staffing to fully support CIP and AT/FP functions from Headquarters down through deploying organizations.
- Pursue funding sources to support adequate staffing of fulltime CIP and AT/FP personnel.

Training and Education.

- CIP is a command responsibility. CIP education and training should be incorporated into current command level courses, as well as courses for senior staff and enlisted personnel.
- Immediately provide our AT/FP officers CIP training and education focused on providing fundamental task understanding and planning guidance.
- Incorporate CIP education and awareness concepts into AT/FP and other appropriate training programs and education to help resolve the shortfall in trained personnel.
- Undertake command level training exercises to simulate attacks (use of Red Teams) to expose vulnerabilities of our critical assets, and incorporate lessons learned.

Funding and Resources.

- Establish long-term programmatic objectives for Marine Corps CIP, both strategic (CIP) and tactical (AT/FP), to include support for education/training.
- Incorporate CIP, AT/FP security requirements in the acquisition and procurement contracting process.
- Establish more comprehensive budget tracking for CIP/AT/FP funding requirements, to include establishing separate Marine Corps program element for CIP program management.

Strategic and Tactical Initiatives.

Critical Asset Identification and Vulnerability Assessment:

- Our immediate and continuing focus must be on the identification and protection of Tier I mission critical infrastructure and assets, which are vital to mission success.
- Develop an integrated and cost-effective framework for a continuing vulnerability assessment process for mission critical assets.
- Formal assessment programs and self-evaluation tools shall be developed, refined and readily accessible on a continuing basis.

Remediation:

- Immediately pursue remediation of mission threatening vulnerabilities to our critical assets and infrastructures identified during the Naval Integrated Vulnerability Assessment (NIVA) process.
- Develop and implement physical security structural upgrade programs for existing facilities housing mission critical assets.
- Relocate USMC mission critical assets from civilian shared tenant spaces into secured USMC or government facilities with appropriate physical security.
- Every installation and base shall develop and maintain a single source document that integrates CIP/AT/FP planning, and provides for periodic update or modification of the integrated plan.

Indications & Warnings:

- Develop and implement a command and control system that will provide the Marine Corps and Navy command centers a realtime, common operating picture with respect to CIP, AT/FP posture, threat monitoring, reporting and decision support, and coordinated security force planning and response activity.
- Support the development of technology initiatives for an integrated I&W capability.
- Establish integrated framework to support timely and consistent reporting of CONUS-based threats to relevant command and CIP activities.
- Support the development of a daily I & W product that fuses all relevant local, regional and national AT/FP, Intel and Law Enforcement data.

Mitigation:

- Support expansion of CBRNE preparedness and response programs.
- Incorporate CIP mitigation strategies in base AT/FP plan.
- Develop and implement CIP-specific post-incident assessments, and capture lessons learned.

- Construct coordinated Crisis/Consequence Management plan, to include the development of a Continuity of Operations Plan (COOP) for assurance of mission critical functions.

Response:

- Undertake installation/base assessment and modeling to determine best mix of “response” equipment and location.
- Establish Military/Civilian Task Forces for Emergency Response where feasible, which define the relationship and synergies of installation ER services with those of outside ER services.
- Establish protocols and response requirements between the armed services.
- Develop and support fully interoperable capability for First Responders communication equipment and mass notification systems.

Reconstitution:

- Formulate an integrated system which will identify reconstitution requirements for continuity of operations, facilitate in the establishment of reconstitution plans, and coordinate the requirements of resource sponsors and the operational chain of command.
- Support DoN/DoD Reconstitution efforts and organizations during crisis management.
- Prepare CIP-specific Reconstitution After-Action Assessments, capturing lessons learned.

Technology Initiatives:

- Utilize and apply working technology solutions to support mission essential functions.
- Support computer based training (CBT) initiatives to provide maximum outreach for CIP, AT/FP basic training and education awareness.
- Seek out and apply the latest technology for secure access to, and transmission of, information and information networks; business processes; and, computer systems.



The Marine Corps must, and will be prepared to successfully defend our Nation against any threat, in any environment, and against any enemy. We have always been successful in the defense of our nation due to the courage, skill and dedication of our Marines, and the availability and use of superior Warfighting assets and systems.

Critical Infrastructure Protection is key to the Marine Corps assuring that our critical Warfighting infrastructures, assets and systems will remain available and in the hands of the men and women defending our Nation.

The initiatives that the Marine Corps is undertaking to protect our mission critical infrastructure must and will meet the conventional and asymmetrical threats of today and tomorrow, whether at home or abroad. We must remain ever vigilant, and constantly adopt our CIP capabilities to changing threats, environment and technology. We must cooperate with and depend upon our commercial partners, civilian agencies, and host nations as never before.



We must, and will lead the way in the development and application of CIP, Anti-Terrorism and Force Protection capabilities in this new battle space. Our ability to deal effectively with terrorism and asymmetrical threats is vital today, and will remain one of our core capabilities for the foreseeable future.

*Protection of our Nation, our critical assets and our Marines is the mission of every Marine – **it is a mission that we must, and will accomplish.***