CIPIS

CRITICAL INFRASTRUCTURE PROTECTION
INTEGRATION STAFF

DOD CRITICAL INFRASTRUCTURE PROTECTION EXECUTION PLAN

CALENDAR YEAR 2000

APPROVED: ____

Richard C. Schaeffer, Jr.
Infrastructure and Information Assurance Directorate

13 March 2000

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 13032000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle DoD Critical Infrastructure Protection Execution Plan. Calendar Year 2000	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) CIPIS	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 24	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** 3/13/00	**3. REPORT TYPE AND DATES COVERED** Report

4. TITLE AND SUBTITLE
DoD Critical Infrastructure Protection Execution Plan

5. FUNDING NUMBERS

6. AUTHOR(S)
Richard C. Schaeffer, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

This document provides a roadmap to be used by the Department of Defense to ensure both an initial operational capability (IOC) and a full operational capability (FOC) for infrastructure assurance. It outlines the CIPIS vision, mission, functions, composition and organizational structure and delineates the goals, objectives, tasks and implementation schedule that are necessary to make effective infrastructure protection a reality within DoD.

14. SUBJECT TERMS
INFRA

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** None

Contents

FORWARD 1

1.1 CIPIS DEFINITION 1

1.2 CRUCIAL ISSUES 2

1.3 CIPIS FOCUS 2

1.4 CIPIS VISION 3

1.5 CIPIS MEANS 3

2. CRITICAL INFRASTRUCTURE PROTECTION INTEGRATION STAFF (CIPIS)........ 5

2.1 CIPIS ORGANIZATION 5

2.2 CIPIS VISION 6

2.3 CIPIS MISSION 6

2.4 CIP REQUIREMENTS 6

2.5 CIPIS FUNCTIONS 7

3. CIPIS GOALS AND IMPLEMENTING ACTIONS 8

3.1 Goal 1 – Ensure the Development of an Integrated CIP Capability 9

3.2 Goal 2 – Foster the Development of Sector Assurance Plans and Special Function Support Plans 14

3.3 Goal 3 - Integrate the Efforts of Other Related DoD Programs into CIP 15

3.4 Goal 4 – Implement a Comprehensive Risk Management Framework to Support CIP 18

3.5 Goal 5 – Establish a Flexible Information Sharing Capability for CIPIS 18

3.6 Goal 6 – Establish Long Term Programmatic Objectives for CIP 20

Figures

Figure 1 - CIP Execution Overview........ 4

Figure 2 – CIPIS Structure 5

Tables

Table 1 – CIPIS Functions 7

Table 2 – CIPIS Goals 8

Table 3 – Critical Infrastructure Protection Activities 9

DoD Critical Infrastructure Protection Execution Plan

FORWARD

The DoD Critical Infrastructure Protection Execution Plan for the Critical Infrastructure Protection Integration Staff (CIPIS) provides the basis for translating requirements set forth in Presidential Decision Directive 63, Critical Infrastructure Protection, DoD Directive 5160.54 Critical Infrastructure Protection (formerly the Critical Asset Assurance Program), the Department of Defense Critical Infrastructure Protection Plan, and the National Plan for Information Systems Protection released by the White House in January 2000. This document provides a roadmap to be used by the Department of Defense to ensure both an initial operational capability (IOC) and a full operational capability (FOC) for infrastructure assurance. It outlines the CIPIS vision, mission, functions, composition and organizational structure and delineates the goals, objectives, tasks and implementation schedule that are necessary to make effective infrastructure protection a reality within DoD.

This plan is a dynamic, living document, reflecting current Department of Defense (DoD) Critical Infrastructure Protection (CIP) policy and program implementation. Therefore changes and course corrections to this Execution Plan will be necessary. The Director, Infrastructure and Information Assurance (I&IA), Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, will ensure that CIPIS makes changes in the Execution Plan to maintain consistency with DoD CIP policy. Such changes will be made to assure that CIPIS carries out DoD CIP policy.

1. EXECUTIVE SUMMARY

1.1 CIPIS DEFINITION

In the context of this Execution Plan, CIPIS is ***an enterprise-wide partnership of organizational entities that are essential for DoD to achieve effective protection of critical infrastructures***. The term infrastructure includes systems and assets that enable the DoD to accomplish its warfighting mission and core business processes. CIPIS leverages CIP efforts of individual organizations, through integrated physical/cyber and on/off-base infrastructure protection strategies, in order to enhance the protection of DoD-mission essential infrastructures upon which the availability and readiness of our military forces depend.

1.1.1 Key Players

Key CIPIS partners include:

- The Office of the Assistant Secretary of Defense (Command, Control, Communications, & Intelligence)
- The eleven Defense Infrastructure (DI) Sectors
- Special Function Components
- The Joint Staff
- The Military Departments and Services and Defense Agencies (including physical and cyber security elements, installations, and system, asset, and infrastructure owners, etc.)
- The Joint Program Office - Special Technical Countermeasures (JPO-STC)
- The Defense Threat Reduction Agency (DTRA)
- The Defense Security Service (DSS)
- The Joint Task Force - Computer Network Defense (JTF-CND); the Defense-wide Information Assurance Program (DIAP); and Service Defensive IO Organizations
- Selected commercial/private sector entities

1.2 CRUCIAL ISSUES

1.2.1 Defining Which Infrastructure Assets are Most Critical

Everything is ***critical*** to someone, but not every asset should be protected to the same degree. To focus on the most critical infrastructure assets, CIPIS will use a tiered view of criticality:

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

1.2.2 Protecting Critical Infrastructures

The concept of ***protecting*** those critical infrastructures necessary to ensure mission success (i.e., vulnerability remediation) focuses initially on single-point failures, and then expands beyond into double-, then triple-point failures. Protection and risk acceptance decisions rest primarily in the hands of infrastructure-owners and installation commanders. ***Successful CIP means influencing these risk acceptance and protection decisions.***

1.3 CIPIS FOCUS

The CIPIS focus is to reduce the risk to DoD strategic military mission accomplishment through a three-step process:

- Enhancing DoD's understanding of critical infrastructure dependencies;
- Mitigating critical infrastructure vulnerabilities; and

- Applying an enterprise-wide risk-based management framework, considering physical and cyber vulnerabilities to government and commercial critical infrastructures, to assist in enterprise-wide, risk acceptance decisions.

The initial emphasis is to identify and mitigate existing Tier I and Tier II vulnerabilities in order to provide the most significant and immediate benefit toward providing military mission assurance and improved operational readiness. As perceived threats and opportunities arise, CIPIS will increase emphasis on the Consequence Management phase of CIP activity. This strategy is consistent with the intent of Presidential Decision Directive (PDD) 63 to ensure critical infrastructure protection and melds well with both the PDD 67 focus on continuity of operations (COOP) and the anti-terrorism emphasis of PDDs 39 and 62.

CIPIS serves to channel OSD focus on CIP into coordinated, enterprise-wide efforts -- facilitating actions of the key players by:

- Assisting in cross-organizational player dialogue
- Providing both context and means for CIP collaboration

1.4 <u>CIPIS VISION</u>

The CIPIS vision is to significantly improve DoD's operational capability and readiness by fully integrating all DoD CIP efforts. For CIPIS to succeed, every DoD infrastructure owner must understand the importance of their critical infrastructures to DoD mission accomplishment, and manage their critical infrastructure dependencies and risk through the conscious application of an enterprise-wide, risk-based management framework.

1.5 <u>CIPIS MEANS</u>

To achieve this vision, CIPIS will develop coordinated physical/cyber and on/off base critical infrastructure protection strategies leveraging a variety of ongoing analyses, assessments, and protection efforts into a coherent, integrated CIP process. This process includes:

- Physical security analyses and assessments;
- Operational security analyses and assessments;
- Anti-Terrorism/Force Protection analyses and assessments;
- Cyber protection and vulnerability analyses and assessments; and
- Off-base commercial infrastructure vulnerability and dependency analyses and assessments.

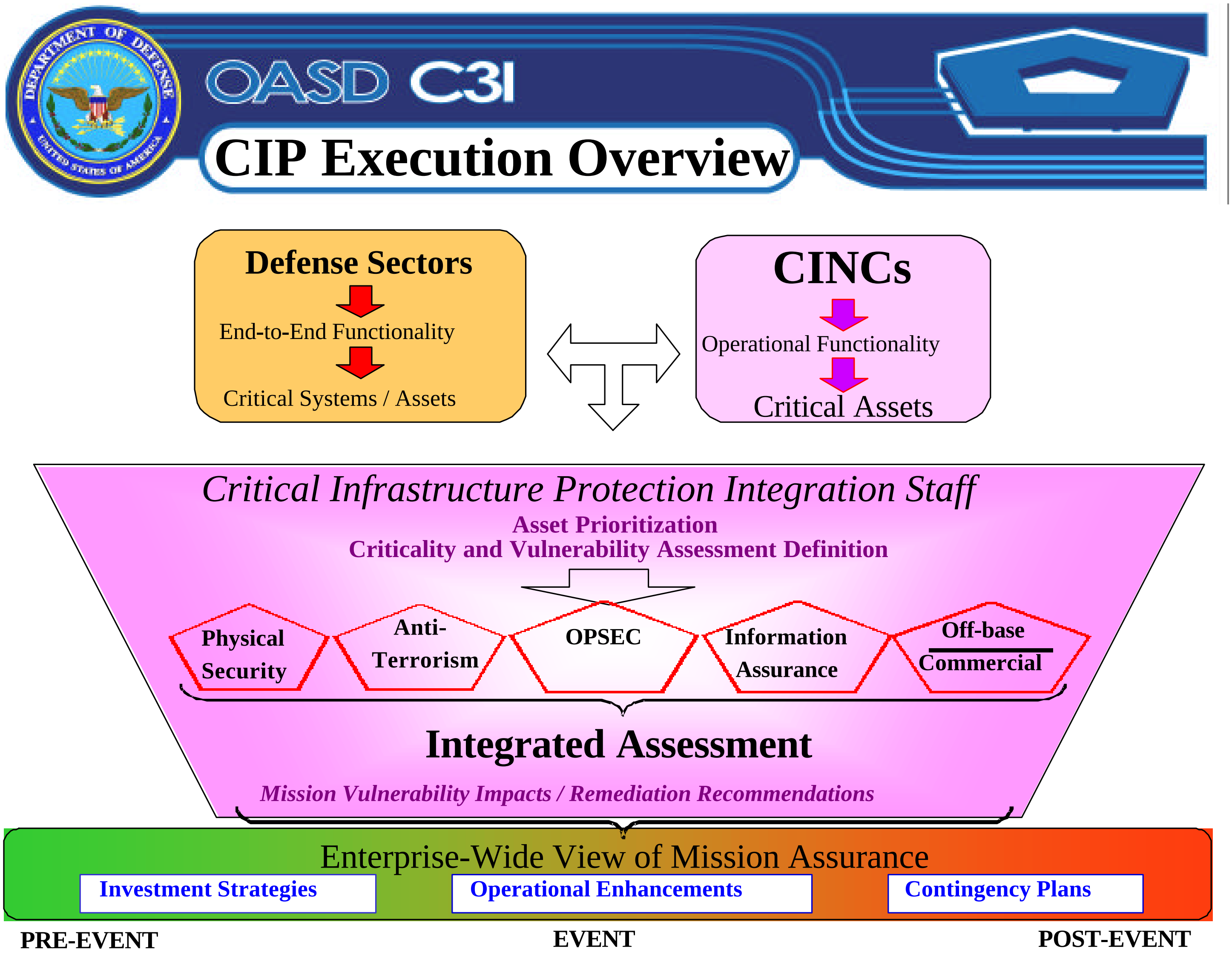

Figure 1 - CIP Execution Overview

2. CRITICAL INFRASTRUCTURE PROTECTION INTEGRATION STAFF (CIPIS)

2.1 CIPIS ORGANIZATION

Under the policy guidance and oversight of the Director, Infrastructure and Information Assurance (I&IA), CIPIS provides a common management environment within which CIP-related programs are planned, coordinated, integrated, and administered. The CIPIS will leverage these programs to assist the Sector Chief Infrastructure Assurance Officers (CIAOs) in the development of Defense Infrastructure Sector Assurance Plans (DISAPs) and the Special Function Coordinators in the development of annual CIP support plans. The CIPIS will support the integration of these plans into an overall integrated DoD CIP plan, coordinated with the Sector CIAOs and submitted to the CIAO Council, and incorporated into deliberate and crisis action planning processes.

CIPIS will be composed of representatives of the DI Lead Agencies, DoD Special Function Agencies, the Joint Staff, Military Services, the CIP Technical Direction Agent (the Joint Program Office for Special Technology Countermeasures (JPO-STC)), and an administrative support staff directed by the CIPIS Coordinator. The CIPIS will serve as a forum for CIP issue coordination. As shown in Figure 1, the DI Sector Lead Agencies will represent the interests of the DoD Components for their particular infrastructure. For example, the Defense Logistics Agency (DLA) will represent the interests of all the Military Services and Defense Agencies as it pertains to the Logistics DI Sector, not just the interests of DLA. The Joint Staff will represent

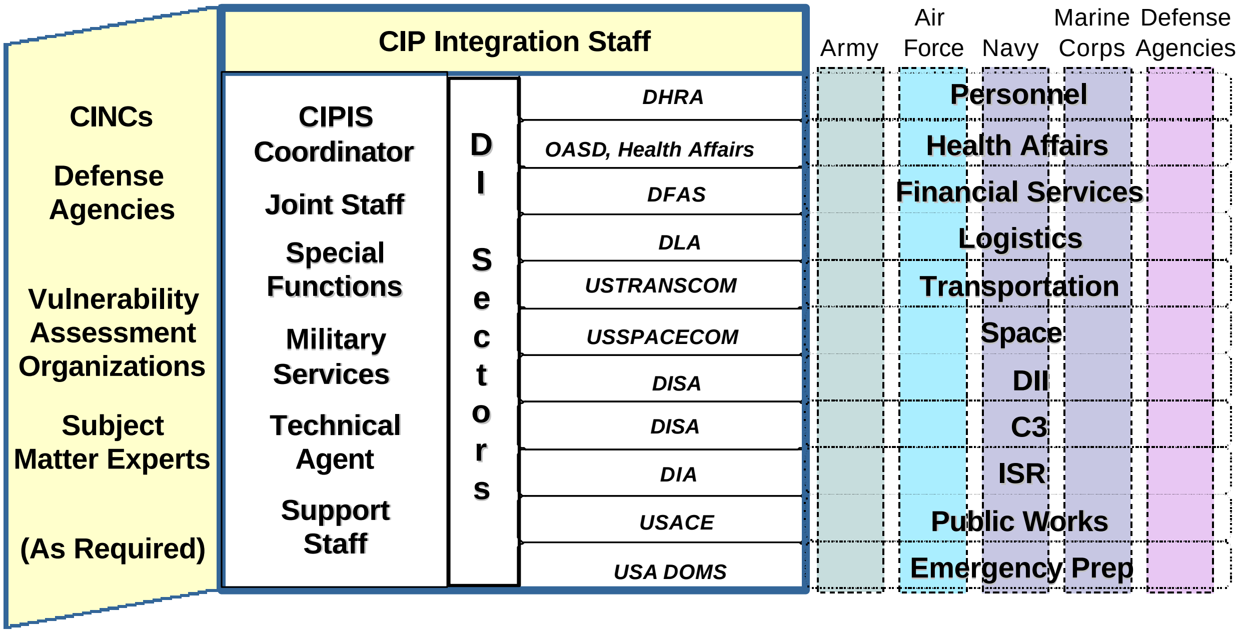

Figure 2 – CIPIS Structure

the interests of the CINCs on routine matters. As circumstances require, CIPIS will request that CINCs, Defense Agencies, vulnerability assessment organizations, and subject matter experts augment the CIPIS on relevant issues. CIPIS members will be "home based" at their parent organization's location, since most of the CIP effort will consist of decentralized execution. While most CIP objectives can be met through virtual collaboration, CIPIS members will meet periodically for centralized planning and issue resolution.

2.2 CIPIS VISION

Significantly improve DoD's operational capability and readiness by fully integrating all DoD CIP efforts.

Today, with fewer systems and assets in the DoD, National, and International infrastructures, which are increasingly interdependent, the availability of key infrastructures directly impact both DoD's Force Readiness and its ability to conduct operations. CIPIS drives the analytical framework for understanding DoD's reliance upon the infrastructures, leverages and integrates existing CIP efforts, and affects a wide range of system enhancements to improve the operating posture of those assets and infrastructures that DoD depends upon for mission accomplishment.

2.3 CIPIS MISSION

Plan, coordinate and integrate the DoD CIP program using a total risk-based management approach to enhance the operational readiness and availability of DoD assets and infrastructures for use by the warfighters and supporting elements.

The CIPIS plans, coordinates and integrates the diverse and distributed elements of the CIP program and other initiatives, seeks to resolve CIP-related issues within DoD, and coordinates (through the OSD CIP Office) with National-level CIP initiatives to assist the warfighters and supporting elements and organizations. It uses a risk-based management approach to affect the wide range of system enhancements aimed at improving the operating posture of those DoD assets and supporting national infrastructures that DoD depends upon for mission accomplishment.

2.4 CIP REQUIREMENTS

Presidential Decision Directive 63 requires every federal department and agency to prepare and implement a plan for protection of its critical infrastructures with a CIP “Initial Operating Capability” (IOC) “not later than the year 2000,” leading to a Full Operating Capability (FOC) for protection of critical infrastructures by 22 May 2003.

2.5 CIPIS FUNCTIONS

Table 1 – CIPIS Functions

CIPIS Functions
Coordinate implementation and execution of the DoD CIP Plan
Assist Sectors and Special Functions in development of Assurance Plans
Coordinate development of an Integrated DoD CIP Assurance Plan
Develop and coordinate the CIP Resource Plan
Facilitate integrated infrastructure analysis, and assessment, and vulnerability remediation
Facilitate CIP Indications and Warning capabilities
Develop and review CIP policy and planning documents
Assist in coordinating Interagency and National level CIP issues

2.5.1 Coordinate Implementation and Execution of the DoD CIP Plan

Due to the diversity of the assets within DoD, uniform execution of the DoD CIP Plan is unrealistic without a central coordinating entity. The CIPIS will serve as the coordinating entity to leverage the knowledge and experiences of CIP across DoD to optimize the program benefits and ensure uniform execution in the interest of mission assurance.

2.5.2 Assist Sectors and Special Functions in Development of Assurance Plans

The CIPIS will provide guidance to assist the Defense Sectors and Special Function components in the development of their Assurance Plans (as required by the DoD CIP Plan). The CIPIS will also assist in the identification of effective and efficient actions and resource investments using a risk-based management approach. The function of the CIPIS in the development of these plans is to minimize the burden on the sectors by providing clear guidance and consistent support.

2.5.3 Coordinate Development of an Integrated DoD CIP Assurance Plan

The CIPIS will lead the effort to integrate the individual DISAPs into an Integrated DoD CIP Assurance Plan. The Plan will describe DoD coordination responsibilities and roles in providing critical infrastructure protection across all the protection activities.

2.5.4 Develop and Coordinate the CIP Resource Plan

The CIPIS works with the participating organizations to identify funding requirements to execute CIP within DoD and enhance its protection measures. These funding requirements can range from supporting initiatives within the DI Sectors and Special Functions to the protection of assets that have been identified as critical to DoD's force readiness and operational capabilities. Once the funding requirements associated with each of the protection activities have been identified, CIPIS prioritizes these funding requirements and presents them to the CIAO Council for concurrence. The CIPIS will produce an annual CIP Resource Plan that provides a complete picture of the funding profiles and requirements of all CIP-related activities in the Department. The CIAO Council will review the CIP Resource Plan and recommend appropriate POM actions.

2.5.5 Facilitate Integrated Infrastructure Analysis, and Assessment, and Vulnerability Remediation

A fundamental requirement of CIP is to understand DoD's reliance upon critical infrastructures. With this requirement in mind, CIPIS will facilitate the analysis of DoD, National and international infrastructures in the context of scenarios and OPLANs to identify critical assets. Once critical assets are identified, DoD assessment efforts will focus on identifying both physical and cyber vulnerabilities to those Department and commercial infrastructures that are critical to military mission success. DoD will then work with asset owners – whether military, government,or commercial – to develop effective vulnerability mitigation efforts focusing on infrastructure protection investment strategies, operational protection enhancements, and contingency plans.

2.5.6 Facilitate CIP Indications and Warning Capabilities

The CIPIS will support ISR Sector and Intelligence Special Function Component leads in identification of requirements and capabilities to develop indications and warning processes and procedures to ensure timely receipt and coordination of information.

2.5.7 Develop and Review CIP Policy and Planning Documents

The CIPIS will coordinate with the DI Sectors to identify issues that require policy clarification, and assist the CIPO in the review and coordination of proposed policy. The CIPIS will develop appropriate planning documents to address these shortfalls. The policy and planning documents described in this function can range from issue papers to rewrites of DoD Directives.

2.5.8 Coordinate Interagency and National Level CIP Issues

Requests for support regarding National-level CIP initiatives will be handled through the CIP Office. The CIPIS will assist the CIP Office on all DoD and national issues pertaining to Critical Infrastructure Protection that require coordination with CIPIS organizations.

3. CIPIS GOALS AND IMPLEMENTING ACTIONS

To fulfill its mission, the CIPIS establishes six broad-based goals. These goals are supported through the achievement of specific objectives and tasks that are detailed in the following sections. For each task, the organizational lead is identified along with an estimated start date, an expected end date, and deliverable where applicable or appropriate.

Table 2 – CIPIS Goals

CIPIS Goals	
Goal 1	Ensure the Development of an Integrated CIP Capability
Goal 2	Foster the Development of Sector Assurance Plans and Special Function Support Plans
Goal 3	Integrate the Efforts of Other Related DoD Programs Into CIP
Goal 4	Implement a Comprehensive Risk Management Framework to Support CIP
Goal 5	Establish a Flexible Information Sharing Capability for CIPIS
Goal 6	Establish Long Term Programmatic Objectives for CIP

3.1 Goal 1 – Ensure the Development of an Integrated CIP Capability

Through review and coordination, CIPIS will ensure balance and compatibility of approaches within each of the protection activities and across DI Sectors. A primary responsibility of the CIPIS is to oversee the full range of CIP protection activities described in Table 3 – Critical Infrastructure Protection Activities. The CIPIS will clearly play an important role in coordinating and, in some cases, leading various elements of the protection activities.

Table 3 – Critical Infrastructure Protection Activities

Protection Activities	Description
Infrastructure Analysis and Assessment	Coordinated identification and characterization of DoD, National, and International critical assets, their system and infrastructure configuration and characteristics, and the intra/interdependencies within and among infrastructure sectors; assessment of their vulnerabilities; quantification of the relationship between military plans and operations and critical assets / infrastructures; and assessment of the operational impact of infrastructure loss or compromise.
Remediation	Deliberate preventative measures undertaken to improve the reliability, availability, and survivability of critical assets and infrastructures (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).
Indications and Warning	Tactical indications through the implementation of sector monitoring and reporting, strategic indications through Intelligence Community support, and warning in coordination with the NIPC in concert with existing DoD and national capabilities.

Protection Activities	Description
Mitigation	Preplanned and coordinated reactions to infrastructure warning and/or incidents designed to reduce or minimize impacts; support and complement emergency, investigation, defense, or other crisis management response; and facilitate reconstitution.
Response	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-CND 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.
Reconstitution	Owner/operator directed restoration of critical assets and infrastructure.

3.1.1 Develop an Integrated Analysis and Assessment Capability

CIPIS will work with the CINCs, Components, DI Sectors, JPO-STC and DTRA to ensure the coordinated development of appropriate models and analytic tools and availability of infrastructure data to supportive the identification of critical assets and interdependency analysis. CIPIS will sponsor the development of a Department of Defense Integrated Vulnerability Assessment (DIVA) process to be used in assessing the criticality and vulnerability of mission essential infrastructure assets.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.1.1	Initially characterize Defense Infrastructures	DI SECTORS	10/99	09/00	Initial Characterization
3.1.1.2	Conduct scenario/operational analysis to identify critical assets	JPO-STC JOINT STAFF SERVICES	10/99	On going	CINC Critical Asset Lists
3.1.1.3	Develop a defense integrated vulnerability assessment (DIVA) process	JPO-STC Joint Staff, Services, DTRA DSS and CIPIS	02/00	08/00	Prototype Standardized Protocol
3.1.1.4	Conduct integrated vulnerability assessments of critical assets	JPO-STC Joint Staff, DSS, DTRA Services	05/00	Ongoing	Integrated Remediation Recommendations
3.1.1.5	Integrate commercial vulnerability assessments	JPO-STC	05/00	On going	Dependency feeds to Assessment Process
3.1.1.6	Integrate information assurance vulnerability assessments	Joint Staff Services DISA	05/00		Dependency feeds to Assessment Process
3.1.1.6	Integrate force protection vulnerability assessments	Joint Staff Services DTRA	05/00	On going	Dependency feeds to Assessment Process

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.1.7	Integrate industrial vulnerability assessments	DSS	05/00	On going	Dependency feeds to Assessment Process
3.1.1.8	Integrate OPSEC assessments	Services DTRA	05/00	On going	Dependency feeds to Assessment Process
3.1.1.9	Characterization of DI Sectors	DI Sectors CIPIS	10/99	On-going	Characterization and Critical Asset List generation

3.1.2 Develop Remediation Measures

CIPIS will facilitate DIVA team efforts to identify and recommended remediation actions that may be taken to improve known deficiencies and weaknesses that could cause a failure or compromise of a critical asset, regardless of whether those events are acts of nature, technology, or malicious actors. DISAPs establish priorities and identify resource requirements for remediation.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.2.1	Conduct mission vulnerability impact assessments	DIVA Assessment CIPIS	05/00	On going	Mission impact assessment to owners.
3.1.2.2	Develop Remediation recommendations	DIVA Assessment CIPIS	05/00	On going	Remediation recommended to asset owners.
3.1.2.3	Assist asset owner implementation efforts when requested	CIPIS Assessment Team	When requested	On going	—

3.1.3 Assist in Establishment of Indications and Warning Reporting Capabilities, Processes and Procedures

CIPIS will support efforts, led by ISR Sector, to establish indication of adversarial capability developed to exploit U.S. vulnerabilities and also implement a structured framework for incident monitoring and reporting. Infrastructure owners and operators are the most likely detectors of changes in infrastructure status and must therefore be considered full partners in the indications process. Indications may result from foreign intelligence, domestic criminal activity, or technical anomalies that indicate system failure or degradation is likely. Innovative fusion of traditional intelligence information with sector monitoring and reporting information is essential for critical infrastructure indications and warning.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.3.1	Identify CIP Indications and Warning requirements	ISR Sector/CIPIS	03/00	12/00	Essential Elements of Information for CIP.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.3.2	Identify current Indications and Warning capabilities	ISR Sector/CIPIS	03/00	12/00	Status Report
3.1.3.3	Develop CIP Indications and Warning reporting processes and procedures	ISR Sector/CIPIS	03/00	12/00	Initial process/procedures.
3.1.3.4	Coordinate with the NMCC, NMJIC, JTF-CND, affected Components, and Defense intelligence community	ISR Sector/CIPIS	03/00	On going	—

3.1.4 Support Development of Mitigation Actions

Mitigation actions are those actions taken by DoD critical asset owners, DoD installations, DI Sectors, and military operators, in response to an infrastructure warning or incident, and are intended to minimize or alleviate the potentially adverse effects on a given military operation or infrastructure, facilitate incident response, and quickly restore the infrastructure service. These actions include measures to safeguard information, gracefully degrade service or shed load in accordance with established priorities, restart equipment or software, or switch to emergency or backup service options. CIPIS will support asset owner development and implementation of mitigation actions.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.4.1	Develop Mitigation recommendations to reduce single point failure impact	JPO-STC DIVA Team Leads	07/00	On going	Mitigation Recommendations
3.1.4.2	Support asset owner development of Mitigation Plan	DIVA team	07/00	On going	Assist owner assistance

3.1.5 Support Development of Incident Response Plans

Response includes those non-owner/operator emergency activities which can assist in eliminating the cause or source of an event and minimize its impact. DI Sectors will address appropriate response measures, to include initial notification and status reporting, are considered and incorporated into Sector planning efforts. CIPIS will facilitate establishment of coordinated reporting mechanisms to ensure timely and accurate reporting.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.5.1	Develop a Response tracking capability (e.g. automated tools).	CIPIS SUPPORT STAFF JPO-STC	08/00	On going	Tracking System
3.1.5.2	Identify Response requirements for Sector business continuity planning	DI SECTORS CIPIS JPO-STC	08/00	On going	Response Requirements for Assurance OPLANS.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.5.3	Coordinate reporting mechanism requirements	CIPIS	08/00	On going	Tools & Mechanisms
3.1.5.4	Coordinate Response requirements (e.g., NMCC, NMJIC, JTF-CD, DOMS and other DoD Response entities) during consequence management	CIPIS	12/99	As required	—
3.1.5.5	Prepare CIP-specific After-Action Assessment requirements	CIPIS	12/99	As required	Report Template

3.1.6 Monitor and Support Reconstitution Efforts

CIPIS will coordinate with the DI Sectors and the Services to ensure that appropriate reconstitution measures are considered and incorporated into Sector and Service planning efforts. CIPIS will facilitate the establishment of reconstitution plans, ensure continuity of operations (COOP) specifics are considered in into reconstitution planning efforts, and support DoD reconstitution entities during crisis management.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.6.1	Identify Reconstitution requirements for Sector business continuity planning	DI SECTORS CIPIS, Services, CINCs.	11/00	On going	Reconstitution Plan requirements
3.1.6.2	Identify Reconstitution requirements for Service continuity planning	SERVICES CIPIS	11/00	On going	Reconstitution Plan requirements
3.1.6.3	Assist in identification of DoD Reconstitution requirements during consequence management	CIPIS	11/00	As required	Reconstitution requirements
3.1.6.4	Incorporate CIP aspects into COOP planning and into Reconstitution planning efforts	DI SECTORS SERVICES CIPIS	12/00	As required	CIP requirement inputs
3.1.6.5	Prepare CIP-specific After-Action Assessment requirements	CIPIS	12/00	As required	Report Template

3.1.7 Integrate CIP Capabilities Across Protection Activities

CIPIS will review the Assurance Plans of each Sector and lead the development of an integrated Assurance Plan for the DoD enterprise.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.7.1	Review the efforts of each Sector within each protection activity	CIPIS	03/00	On going	—
3.1.7.2	Conduct gap and compatibility analysis	CIPIS	04/00	On going	Sector recommendations
3.1.7.3	Prepare recommendations for integrated plan	CIPIS	05/00	On going	Input to draft Integrated Assurance Plan

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.1.7.4	Continuous review of Sector protection activity integration	CIPIS	09/00	As required	—

3.2 Goal 2 – Foster the Development of Sector Assurance Plans and Special Function Support Plans

CIPIS will support the development of defense sector and special function plans through guidance and the coordinated leveraging of developments and lessons learned from other efforts in the overall CIP effort.

3.2.1 Develop Planning Guidance for Sector Assurance Plans

CIPO will provide policy guidance. CIPIS will facilitate coordination between CIP Office and the DI Sector Lead Components to develop planning guidance in the context of national guidance and the DoD CIP, regarding development of the DISAPs.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.2.1.1	Review existing guidance	CIP Office	11/99	11/99	—
3.2.1.2	Identify gaps and deficiencies	CIP Office	11/99	11/99	—
3.2.1.3	Develop and coordinate draft guidance	CIPO CIPIS	11/99	11/99	Draft Guidance
3.2.1.4	Distribute Sector Assurance Plan guidance	CIPO CIPIS	12/99	01/00	Final Guidance
3.2.1.5	Develop Sector Assurance Plan Guidance for follow on plans	CIPO CIPIS	06/00	On going	Follow on Guidance

3.2.2 Support Sectors in Developing Sector Assurance Plans

CIPIS will work with the DI Sectors and JPO-STC to ensure a coordinated approach to Sector characterization and the development of Sector Assurance Plans.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.2.2.1	Assist the DI Sectors in developing their DISAPs	CIPIS	10/99	01/00	Initial submission
3.2.2.2	Continue to assist Sectors in DISAP development	CIPIS	01/00	On going	Revised Plans

3.2.3 Develop an Integrated DoD CIP Assurance Plan

CIPIS will review and incorporate the various DISAPs into an Integrated DoD CIP Plan.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.2.3.1	Develop and coordinate initial Integrated Assurance Plan	CIPIS	04/00	08/00	Initial Plan
3.2.3.2	Continue development of Integrated Assurance Plan	CIPIS	09/00	On going	Follow on Plan

3.2.4 Develop Planning Guidance for Special Function Support Plans

CIPIS will facilitate the coordination between CIP Office and the Special Function Lead Components in the development of planning guidance, in the context of national guidance and the DoD CIP, regarding development of the Special Function Support Plans.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.2.4.1	Review existing guidance	CIPO CIPIS	04/00	04/00	—
3.2.4.2	Identify gaps and deficiencies	CIPO CIPIS	05/00	05/00	—
3.2.4.3	Develop and coordinate draft guidance	CIPO CIPIS	05/00	08/00	Draft Guidance
3.2.4.4	Distribute Special Function Support Plan guidance	CIPO CIPIS	07/00	09/00	Final Guidance

3.3 Goal 3 - Integrate the Efforts of Other Related DoD Programs into CIP

CIPIS will serve as the central coordinating point to ensure consistent approaches are employed in all DoD CIP-related efforts. The CIPIS will leverage and integrate these efforts for improved support to the DI Sectors and the Military Operator community.

3.3.1 Identify Opportunities from the Year 2000 (Y2K) Efforts

CIPIS will review the Year 2000 (Y2K) efforts to capitalize on the unique concepts, data, tools, and techniques that might be leveraged in support of the overall CIP efforts.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.1.1	Review program	CIPIS	10/99	03/00	—

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.1.2	Identify concepts and capabilities to leverage	CIPIS	01/00	04/00	CIP recommendations

3.3.2 Identify opportunities from the Infrastructure Assurance Program

CIPIS will review the Infrastructure Assurance Program to capitalize on the unique concepts, data, tools, and techniques that might be leveraged in support of the overall CIP efforts.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.2.1	Review program	CIPIS	05/00	08/00	—
3.3.2.2	Identify t concepts and capabilities to leverage	CIPIS	08/00	11/00	CIP recommendations

3.3.3 Identify Opportunities from the Defense-wide Information Assurance Program

CIPIS will review the Defense-wide Information Assurance Program to capitalize on the unique concepts, data, tools, and techniques that might be leveraged in support of the overall CIP efforts.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.3.1	Review program	CIPIS	05/00	08/00	—
3.3.3.2	Identify t concepts and capabilities to leverage	CIPIS	08/00	11/00	CIP recommendations

3.3.4 Identify Opportunities from the Anti-Terrorism / Force Protection Programs

CIPIS will review existing Anti-Terrorism / Force Protection Programs to capitalize on the unique concepts, data, tools, and techniques that might be leveraged in support of the overall CIP efforts.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.4.1	Review program	CIPIS	10/99	08/00	—
3.3.4.2	Identify concepts and capabilities to leverage	CIPIS	01/00	11/00	CIP recommendations

3.3.5 Identify Opportunities from the Continuity of Operations Programs

CIPIS will review the Continuity of Operations Programs to capitalize on the unique concepts, data, tools, and techniques that might be leveraged in support of the overall CIP efforts.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.5.1	Review program	CIPIS	05/00	08/00	—
3.3.5.2	Identify concepts and capabilities to leverage	CIPIS	08/00	10/00	CIP recommendations

3.3.6 Identify opportunities from the Information Operations Programs

CIPIS will review the Information Operations programs to capitalize on the unique concepts, data, tools, and techniques that might be leveraged in support of the overall CIP efforts.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.6.1	Review program	CIPIS	05/00	06/00	—
3.3.6.2	Identify concepts and capabilities to leverage	CIPIS	06/00	07/00	CIP recommendations

3.3.7 Prepare Recommendations for Integration

CIPIS will consolidate the capabilities identified in Tasks 3.3.1 through 3.3.6 into a time-phased, prioritized list of recommendations.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.7.1	Develop list of recommendations	CIPIS	08/00	12/00	Briefing

3.3.8 Monitor Implementation

CIPIS will work closely with the DI Sectors and the CIPO to monitor the implementation of the decisions made by the CIAO Council, and will prepare periodic status reports.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.3.8.1	Plan for the implementation of the CIAO Council's decisions	CIPIS	10/00	02/01	Plan
3.3.8.2	Monitor implementation progress	CIPIS		On going	—

3.4 Goal 4 – Implement a Comprehensive Risk Management Framework to Support CIP

The CIPIS will use a comprehensive risk management framework to review the vulnerabilities of DI Sectors. The framework will assist in identifying, measuring, quantifying, and evaluating the probability and risks of a critical asset being unavailable, as well as the consequences and impacts on DoD missions, based on the project-specific scales of criticality. Recommended options and their associated trade-offs in terms of costs, benefits, and risks can then be made. The output of the risk management framework will assist in the development the CIP Resource Plan.

3.4.1 Develop a CIP Risk-based Management Framework and Methods

CIPIS will develop a CIP risk-based management framework for the identification, measurement, and evaluation of the probability, risk, and consequences associated with the unavailability of a critical asset. Implementation and execution will be reviewed to provide feedback for future refinements to the methodologies.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.4.1.1	Initiate industry study	JPO-STC	09/99	06/00	Industry summary
3.4.1.2	Review and identify risk-based management frameworks/methodologies across DI sectors	JPO-STC DI Sectors	04/00	09/00	—
3.4.1.3	Prepare recommendations for a CIP risk management framework and methods	JPO-STC	09/00	12/00	Recommendations
3.4.1.4	Formalize CIP risk-based management framework and methodologies and brief CIAO Council	CIPIS	09/00	03/01	Briefing
3.4.1.5	Incorporate CIAO Council decision into CIP Plan	CIPO	04/01	On going	—

3.5 Goal 5 – Establish a Flexible Information Sharing Capability for CIPIS

To achieve its mission in a timely and effective manner, the CIPIS will identify user requirements for sharing information and develop a concept and an architecture to facilitate information sharing and coordination throughout participating and affected DoD organizations.

3.5.1 Develop a CIPIS Information Management Construct to Enable Information Sharing

CIPIS will develop a concept to promote information sharing among all affected DoD elements. This will include sharing of CIP information between and among those stakeholders that are part of the CIP program (including those who execute military operations, others who use DOD's infrastructures and support those who execute military operations, and those who own DI assets and contract for commercial support), but also between all CIP program stakeholders and the private sector owners and operators of infrastructure critical to the DoD's successful performance of strategic missions. CIPIS will identify requirements and develop strategies to establish and maintain liaison relationships with owners and operators of infrastructure assets to increase information flow and facilitate cooperation between CIPIS and other organizations. CIPIS will assist government and private sector partners in developing infrastructure protection training needs, curricula, and materials.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.5.1.1	Develop an internal information sharing concept	CIPIS	09/99	04/00	Concept document
3.5.1.2	Develop internal requirements	CIPIS	03/00	05/00	Requirements
3.5.1.3	Design CIPIS information management construct	CIPIS	05/00	12/00	Information management construct
3.5.1.4	Implement CIPIS information management construct	CIPIS	12/00	On going	—
3.5.1.5	Review information sharing needs, from the installation to the CIP program stakeholder level	CIPIS	06/99	On going	Inputs to construct
3.5.1.6	Review other existing information sharing models	CIPIS	06/99	05/00	Inputs to construct
3.5.1.7	Manage CIP program information sharing.	CIPO	01/00	On going	—

3.5.2 Develop CIPIS Security Management Plan

CIPIS will provide inputs and support CIP Office in the development of the CIPIS security management plan that delineates the roles, responsibilities, and instructions for implementing and maintaining the security policies and procedures of the program.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.5.2.1	Develop requirements	CIPO	11/99	04/00	Requirements
3.5.2.2	Coordinate plan	CIPO	03/00	06/00	Security Management Plan

3.5.3 Provide CIPIS Planning Support (Annual Plan, Resource Plan)

CIPIS will identify issues and coordinate with CIP Office in the development of planning documents that provide implementation guidance to the key players and will address such activities as asset data collection, vulnerability assessments, infrastructure dependency analysis, exercise plans and scenario generation, and resources. CIP activity will tend to change on an annual basis depending on a number of factors including end user requirements, the changing threat environment, and current operations within the Department.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.5.3.1	Develop requirements	CIPO	12/99	On going	Requirements
3.5.3.2	Coordinate plans	CIPO	02/00	On going	Plans

3.5.4 Define and Establish a CIPIS Administrative Support Staff

CIPIS will establish a dedicated support staff to provide for administrative coordination and support for CIPIS activities.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.5.4.1	Identify requirements	CIPIS	01/00	08/00	Requirements
3.5.4.2	Initiate personnel/contracting actions	CIPIS	08/00	12/00	Support actions
3.5.4.3	Manage CIPIS Support Staff	CIPIS		On going	—

3.6 Goal 6 – Establish Long Term Programmatic Objectives for CIP

CIPIS will support the CIAO Council through the development of recommendations for long- term CIP objectives and to support the institutionalization of the CIP process. CIPIS recommendations shall be reviewed by DI Sectors prior to submission to the CIAO Council.

3.6.1 Integrate CIP into the Planning, Programming, and Budgeting Process

CIPIS will work with the DI Sectors to identify programmatic issues and recommendations to support CIP Planning, Programming and Budgeting System efforts. CIPIS will provide CIPO with rationale to support decision making and the defense of CIP funding for analysis and assessment of infrastructure interdependencies in order to support continuity planning, security, and protection.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.6.1.1	Conduct periodic reviews	CIPIS	12/99	On going	—
3.6.1.2	Develop programmatic issues	CIPIS	02/00	On going	Issue Papers
3.6.1.3	Participate in PPBS process	CIPO	02/00	On going	—

3.6.2 Develop Recommendations for Long Term CIP Program Objectives

CIPIS will coordinate with the DI Sectors and CIP Office to develop recommendations for long term CIP program objectives to support planning, investment, and operations.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.6.2.1	Identify potential long term objectives	CIPIS	12/99	On going	Objectives
3.6.2.2	Identify resource requirements	CIPIS	02/00	On going	Requirements
3.6.2.3	Develop priorities	CIPIS	03/00	On going	Priorities
3.6.2.4	Develop recommendations for CIAO Council consideration	CIPIS	03/00	On going*)*	Briefing

3.6.3 Institutionalize Findings and Recommendations

CIPIS will present its findings and recommendations to the CIAO Council for approval, following DI Sector review, to ensure a consistent and coherent approach that is supported by DoD leadership for Department-wide implementation.

CIPIS TASK AREA	ACTION	RESPONSIBILITY	START DATE	END DATE	DELIVERABLE
3.6.3.1	Develop Integrated DoD CIP Assurance Plan for approval	CIPIS	03/00	06/00	Briefing
3.6.3.2	Provide recommendations for leveraging capabilities from related programs	CIPIS	03/00	11/00	Briefing
3.6.3.3	Present CIPIS security management plan for approval	CIPIS	11/99	06/00	Briefing
3.6.3.4	Present outreach and training support plan for approval	CIPIS	04/00	11/00	Briefing