Defense Critical Infrastructure Program Integrated Enterprise Architecture

All Views (AV-1) Overview and Summary Information

Version 1.0

June 30, 2006

DCIP Integrated Enterprise Architecture

All Views (AV-1) Overview and Summary Information

Revision Sheet

Version No.	Date	Revision Description
1.0	June 30, 2006	Final version

DCIP Integrated Enterprise Architecture
All Views (AV-1) Overview and Summary Information

Table of Contents

List of Tables

List of Figures

DCIP Integrated Enterprise Architecture
All Views (AV-1) Overview and Summary Information

1 BACKGROUND

The Department of Defense (DoD) defines the Defense Critical Infrastructure Program (DCIP) as "A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.[1]" The current method of providing situational awareness is through a linear process consisting primarily of data calls. This method frequently produces inconsistent data resulting from differing interpretations of the requirements and is inefficient at best. Implementing DCIP requires the community to become fully integrated concerning process and information sharing.

The DCIP Integrated Enterprise Architecture (IEA) is the enabling framework for information sharing for risk management of critical assets. This framework captures the business requirements and information needs necessary to make astute informed decisions about technology, policy, procedures, organization, personnel training, and operations for risk management.

The single most important product of the DCIP IEA initiative is the set of Shared Data Environment Metadata Definitions and the technical specifications that the DCIP community will use to modify their systems to enable the information sharing that is critical to accomplishment of the DCIP mission. This information sharing will minimize the data calls that are currently being used to gather, collate, analyze, disseminate, and support decision-making. The net gain through improved and seamless information sharing is significantly reduced cost to operate DCIP, improved responsiveness to senior leadership, and improved infrastructure resiliency.

This document, the Overview and Summary Information (AV-1), states the assumptions, constraints, and limitations that may affect high-level decision processes involving this architecture.

2 ARCHITECTURE PROJECT IDENTIFICATION

Name	DCIP Enterprise Architecture
Architect	Antwane V. Johnson Deputy, DCIP (Enterprise Architecture)
Organization Developing the Architecture	Office of the Assistant Secretary of Defense Homeland Defense (ASD HD)
Approval Authority	Office of the Assistant Secretary of Defense Homeland Defense (ASD HD)
Date Completed	June 2006

[1] DoD Directive 3020.40, pg. 9

2.1 Assumptions

- Architectural work developed within the DCIP community will be leveraged and re-used amongst community members
- Views will only be prepared where they directly support DCIP stakeholder needs and solutions
- Department of Defense Directive 3020.40 "Defense Critical Infrastructure Program (DCIP)" is the policy authority
- The Interim Implementation Guidance provided significant input to both the Transition and Target Architectures

2.2 Level of Effort, Projected Costs and Actual Costs to Develop the Architecture

Phase	Level of Effort / Projected Costs	Level of Effort / Actual Costs
I – Baseline Characterization	3.4 FTE / $599,785	4 FTE / $599,785
II – Target Architecture	2.9 FTE / $499,951	3.6 FTE / $499,951
III – Solutions	TBD	

2.3 Phases

Phase	Description
I – Baseline Characterization	Identification of DCIP stakeholder needs and requirements. High-level depiction of the current DCIP environment. Establishment of EA governance and EARB processes. Linkage between EA and portfolio management.
II – Target Architecture	Development of the Target Architecture that satisfies the business requirements for information sharing and risk management
III – Solutions	Implementation of specific solutions (prioritized) to achieve the Target Architecture, including organizational initiatives required to improve DCIP operations. Increased use of the IEA as a tool for portfolio and governance decisions.

3 SCOPE: ARCHITECTURE VIEWS(S) AND PRODUCT IDENTIFICATION

The DCIP IEA leverages the principles of the DoDAF to provide a core set of products and views that define DCIP business needs and point to solutions. Several of the views, e.g., OV-2, OV-3, and OV-5 are being developed as Transition views to support DCIP near-term needs. The products and views included in the DCIP IEA are shown in Table 1.

Table 1 - DoDAF Products used by DCIP

Reference	Architecture Product
AV-1	Overview and Summary
AV-2	Integrated Dictionary
OV-1	High-level Operational Concept Description
OV-2*	Operational Node Connectivity Description
OV-3	Operational Information Exchange Matrix
OV-5*	Activity Model
SV-1	System Interface Description – in context of solutions only
SV-5	Operational Activity to System Functionality Matrix
SV-8	System Evolution Description
SV-9	System Technology Forecast
TV-1	Technical Standards Profile
	* The OV-2 and the OV-5 were combined to simplify the presentation of the business rules and performers.

Though the IEA development and implementation activities will be generally shortlived, DCIP will continue to provide the long-term foundation for DoD situational awareness, risk management, and decision support.

3.1 Time Frames

Phase	Timeframe
I – Baseline Characterization	April 2005 – December 2005
II – Target Architecture	December 2005 – June 2006
III – Solutions	July 2006 – Ongoing

3.2 Organizations Involved

The organizations involved in the DCIP program as defined in Department of Defense Directive (DODD) 3020.40 are:

- Under Secretary of Defense for Policy (USD(P))
    - Assistant Secretary of Defense for Homeland Defense (ASD(HD))
    - Assistant Secretary of Defense for International Security Policy (ASD(ISP))
- Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))
- Under Secretary of Defense for Intelligence (USD(I))

- Under Secretary of Defense Comptroller/Chief Financial Officer (USD(C)/CFO)
- Under Secretary of Defense for Personnel and Readiness (USD(P&R))
- Assistant Secretary of Defense for Networks & Information Integration (ASD(NII))
- Chairman of the Joint Chiefs of Staff (CJCS)
- Commanders of the Geographic Combatant Commands
- Commanders of the Functional Combatant Commands
- Secretaries of the Military Departments, the Commander, U.S. Special Operations Command, the Chief, National Guard Bureau (in coordination with the National Guard Adjutants General of the States), and the Directors of Defense Agencies and DoD Field Activities
- Defense Sectors Lead Agencies

Defense Industrial Base (DIB)	Director, Defense Contract Management Agency
Financial Services	Director, Defense Finance & Accounting Service
Global Information Grid (GIG)	Director, Defense Information Systems Agency
Health Affairs	Assistant Secretary of Defense for Health Affairs
Intelligence, Surveillance, and Reconnaissance (ISR)	Director, Defense Intelligence Agency
Logistics	Director, Defense Logistics Agency
Personnel	Director, DoD Human Resources Activity
Public Works	Chief of Engineers and Commander, U.S. Army Corps of Engineers
Space	Commander, U.S. Strategic Command
Transportation	Commander, U.S. Transportation Command

4 PURPOSE AND VIEWPOINT

The purpose of the DCIP IEA is to describe the framework for enabling information sharing for risk management of critical assets. This framework captures the business requirements and information needs required to make informed decisions about technology, policy, procedures, organization, personnel training, and operations for risk management. These architecture products help ensure a common denominator for understanding, comparing, and integrating infrastructure alternatives. The DCIP IEA is designed to support the following activities:

- Strategic Planning
- Performance Management
- Portfolio Management
- Planning, Programming, Budgeting, and Execution (PPBE)
- Enterprise Programs / Project Management
- Performance Metrics
- Process Improvement

The DCIP IEA is following a best-practice approach of using the issues and needs of its stakeholder community to identify architecturally based solutions that address the requirements and information needs to support the above activities. Examples of the business activities addressed by the DCIP IEA include, but are not limited to:

- **Identification of Assets –** The IEA provides DCIP stakeholders with the ability to re-use asset characterization and identification capabilities.
- **Interdependency of Assets –** The IEA identifies capabilities within the DCIP community that can relate common assets. The IEA enables the implementation of a standard set of interdependency constructs, i.e., the use of JMETS to link assets.
- **Risk Assessments of Assets –** The IEA provides a framework for managing risk assessments and identifies the information needed to capture, document, and make decisions to reduce risk
- **Risk Response –** The IEA provides frameworks for making decisions about risk remediation, risk mitigation, and capability reconstitution. Additionally, it describes the processes to be used in reporting response actions.
- **Management of Resources –** The IEA provides DCIP policy and decision makers with a framework by which they can make resource and governance decisions. The IEA enables decision makers to evaluate a request for resources against the current available capabilities and the future capabilities.
- **Sharing of Information –** The IEA, through its foundation of net-centric shared data, will define common processes for all aspects of the DCIP core activities. The common processes provide the framework by which information regarding assets, their vulnerabilities, and risk mitigation options can be shared.

4.1 Viewpoint

The DCIP IEA is being prepared from the viewpoint of the DCIP community members who need to share information to accomplish their DCIP missions of risk assessment, management, and response. The business processes captured in the OV-2/5 views are oriented to these missions and the information and data needs defined in the OV-3 as decomposed into individual Information Exchange Requirements maintain this orientation. By integrating the net-centric Shared Data Environment throughout the IEA, DCIP clearly focuses on the future of information sharing as defined by the Net-Centric Operations and Warfare Reference Model (NCOW).

5 CONTEXT

5.1 DCIP Vision / Mission

The DCIP IEA was developed with an emphasis on transforming the program and identifying the business, system, and technical capabilities required to achieve the DCIP vision and mission, enable information sharing, and address stakeholder needs. The Target IEA is focused on key transition initiatives required to implement the DCIP vision; *"Global Defense Infrastructure Resiliency"* and mission; *"Support decision makers at all levels with timely, high quality recommendations to ensure that defense critical infrastructure is available when required."*

In order to accomplish its mission and to achieve its vision, it is imperative for DCIP to acquire and maintain an ongoing, preferably real-time, situational awareness of the risks to DCIP assets across the entire DoD Enterprise. This includes those assets not owned or controlled by the Government, but which are essential to providing support to DoD's strategic mission. The DCIP IEA describes the activities and information required to develop and employ a risk-based approach for management of assets critical to DoD missions. Ensuring availability requires that military commanders understand which assets are critical, which assets are vulnerable, and what risk mitigation options are available in context of asset availability.

5.2 DCIP IEA Goals

In order to provide warfighters and decision makers with the ability to manage risks by identifying what is critical, determining vulnerabilities, and taking actions to reduce risk, the DCIP IEA focuses on developing executable solutions centered around the DCIP core activities: Analysis and Assessment, Remediation, Mitigation, and Reconstitution. The goals pursued by the DCIP IEA in support of executable solutions include:

- Architecture – Provide a needs-based DoDAF compliant architecture
- Policy – Integrate the DCIP IEA with other DoD EA programs. Utilize the IEA as a means to influence the governance and portfolio management processes
- Strategy and planning – Utilize the IEA as a tool to identify missing DCIP capabilities and information, and the associated strategic and transition planning guidance
- Financial – Utilize the IEA as a tool to enable DCIP decision makers to evaluate and prioritize resource requests
- Human resources – Promote the value of IEA through education, training, and outreach
- Technical capabilities – Utilize the IEA to establish a set of common technical standards and capabilities

5.3 DCIP IEA Objectives

The objectives of the DCIP IEA are shown in Table 2.

Table 2 - DCIP IEA Objectives

Objective Category	Specific Objectives
Architecture	• Integrate with the Net-Centric Environment • Identify and address capability gaps • Develop the appropriate EA artifacts necessary to provide solutions to DCIP needs
Policy	• Ensure DCIP alignment with the PMA, GIG, BEA, and NCOW RM • Ensure common IEA policy and guidance across the DCIP community • Ensure the Target IEA aligns with other DoD and OMB frameworks/models • Ensure the DCIP IEA Policy is complementary with and/or leverages the existing EA policies of other DoD organizations, where appropriate
Financial	• Ensure DCIP investments are related and complementary across the DCIP community

Objective Category	Specific Objectives
Technical Capabilities	• Ensure a standards-based technical strategy and portfolio • Ensure a uniform standards adoption across all DCIP projects • Promote the use of new and innovative technologies, as appropriate

5.4 Concept of Operations

The DoD, through the DCIP community, has missions to perform risk management to protect critical infrastructure assets. Additionally, it has requirements to create enterprise architectures. As illustrated in Figure 1, the DCIP IEA is the framework that describes the information needed for strategic decisions on resource allocation and prioritization within the Office of the Secretary of Defense and for accomplishing the DCIP Mission.

To accomplish these goals, the IEA describes a DCIP Shared Data Environment to leverage the power of the net-centric GIG and enable the DCIP community to share data. This key enabling concept leverages the data available from DCIP support systems to enable decision makers across the community to view the data they need.

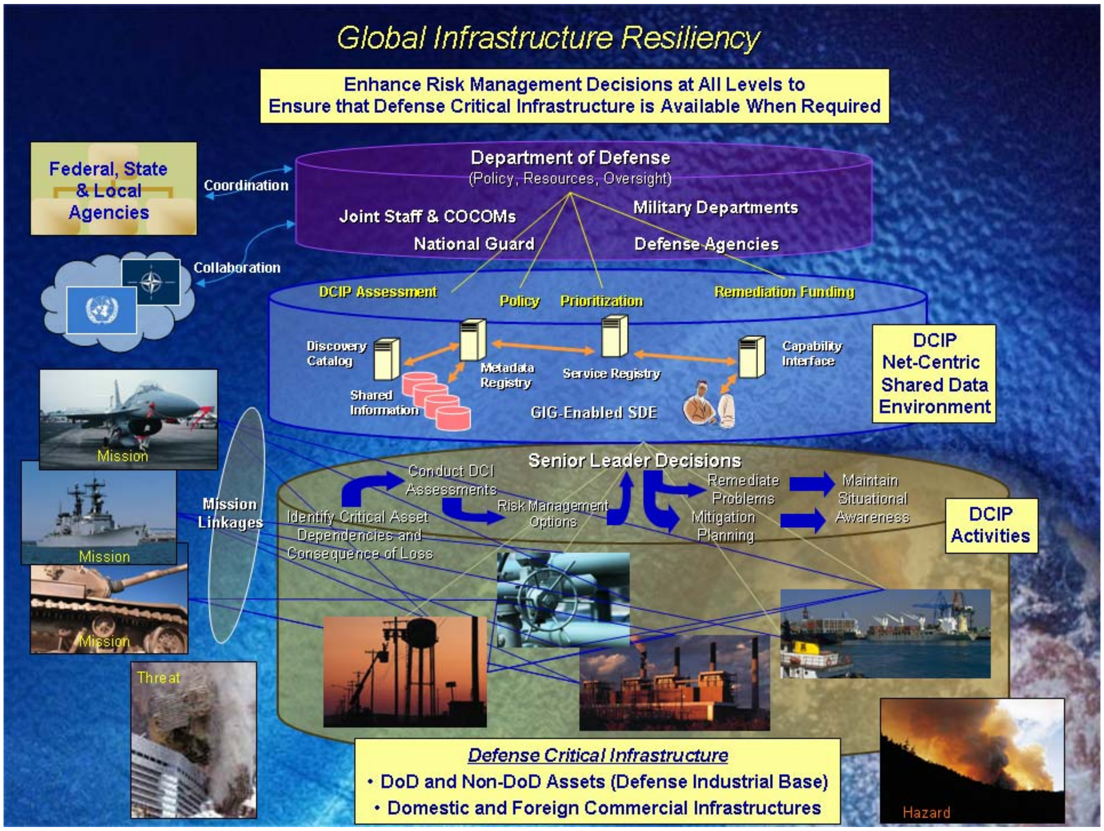
Global Infrastructure Resiliency
Enhance Risk Management Decisions at All Levels to Ensure that Defense Critical Infrastructure is Available When Required
Federal, State & Local Agencies
Coordination
Collaboration
Department of Defense
(Policy, Resources, Oversight)
Joint Staff & COCOMs
Military Departments
National Guard
Defense Agencies
DCIP Assessment
Policy
Prioritization
Remediation Funding
Discovery Catalog
Metadata Registry
Service Registry
Capability Interface
Shared Information
GIG-Enabled SDE
DCIP Net-Centric Shared Data Environment
Mission
Mission
Mission
Mission Linkages
Threat
Senior Leader Decisions
Conduct DCI Assessments
Identify Critical Asset Dependencies and Consequence of Loss
Risk Management Options
Remediate Problems
Mitigation Planning
Maintain Situational Awareness
DCIP Activities
Defense Critical Infrastructure
• DoD and Non-DoD Assets (Defense Industrial Base)
• Domestic and Foreign Commercial Infrastructures
Hazard

Figure 1 - DCIP Conceptual Diagram

During normal day-to-day operations, the Shared Data Environment will provide visibility of the information necessary to develop policy and make informed decisions for properly allocating resources for risk management. For example, during the asset interdependency analysis phase, many organizations need to collaborate and make decisions on dependencies. By accessing the shared information via the capability interface, service registry, and shared services, each will be able to contribute to the ultimate decision. The capability interface provides users with access to the environment and visibility of the data they are authorized to see. The combination of the service and metadata registries points the capability interface to the right data sources. As another example, in a post-event response scenario, senior decision-makers will be able to monitor the status of mitigation activities and make decisions needed for allocation of resources.

The major benefit of this approach is situational awareness of all aspects of DCIP from policy development to risk management and response.

5.4.1 Enabling initiatives

Enabling transition initiatives represent the activities that should be undertaken within the DCIP community to implement the architecture. The transition initiatives are specific activities that generate solutions to stakeholder needs and improve the community's overall ability to execute the DCIP mission. The primary enabling transition initiatives are listed in Table 3, and are identified as either Organizational ("O-*nn*") or Technical ("T-*nn*") Initiatives.

Table 3 - Transition Initiatives

Transition Initiative
O-01 Define and Assign Executive Agent Activities
O-02 Establish a Community of Interest
O-03 Develop a Strategy for Budget Advocacy
T-01 Define DCIP Metadata Definitions
T-02 Implement DCIP Shared Data Environment Interface
T-03 Implement an Asset Registration Service
T-04 Implement the Asset Identification and Prioritization Service
T-05 Implement the Asset Assessment Service
T-06 Implement Use Services

5.5 Rules, Criteria, Conventions Followed

The DCIP IEA was built following the framework methodology of the DoDAF v 1.0, with the modification that the OV-2, Operational Node Connectivity Chart and OV-5, Operational Activity Model Chart have been combined into a single product, OV-2/5. This combined product permits viewers to gain an overall understanding of the DCIP information flows and activity interactions in a single document.

The IEA depicts the processes applicable to DCIP derived from several governing documents including Homeland Security Presidential Directive 7, DoD Directive 3020.40, and the DCIP Interim Implementation Guidance. Additionally, the Target Architecture conforms to the Net Centric Operations and Warfare Reference and Global Information Grid Operations Models as closely as possible. As these two models evolve, the DCIP IEA will necessarily change to conform where possible, with deviations kept to the minimum needed to execute the business processes required by DCIP-specific direction from higher authority.

5.6 Linkages to Other Architectures

The DCIP IEA is developed as a net-centric architecture. In implementation, each DCIP community member will be able to link their architecture models to the DCIP Net-Centric Shared Data Environment. The DCIP IEA is intended to be published on the Critical Infrastructure Protection Integration Staff (CIPIS) web site in order to provide universal access to all DCIP stakeholders.

6 TOOLS AND FILE FORMATS USED

Products are being developed using Proforma ProVision Modeling Suite, Microsoft Visio, and Microsoft Office applications. Final products will be available in Adobe PDF and standard Microsoft Office file formats.

eRoom is being used as a collaboration and management workspace for sharing information. eRoom is a web based electronic collaboration site maintained by Documentum with SuprTEK administering the DCIP community rooms..

Terminology used in DCIP IEA artifacts and work products, including this document, can be referenced in the All Views (AV) –2 Integrated Dictionary.

7 FINDINGS

7.1 Analysis Results

Development of the DCIP IEA has lead to the discovery of a number of program challenges that are typical in relatively new programs. Additionally, the strong emphasis in cross organizational information sharing both within DoD, with other Federal, state and local government entities, and with private sector assets, as a result of the Hurricane Katrina experience has added additional impetus to defining and implementing a net-centric solution, as documented in the IEA. Table 4 illustrates some of the challenges identified during development of the IEA.

Table 4 - Gap Analysis Results

ID	Current State	Gap
1.	While the role of ASD (HD) DCIP is policy, oversight and budget advocacy, it has been performing a number of operational DCIP responsibilities in order to move the nascent program forward.	An appropriate operational arm to manage the DCIP for ASD (HD) DCIP needs to be identified and implemented.
2.	DCIP is a relatively new program with high visibility when events such as Hurricane Katrina occur. Senior leadership has expressed frustration with the lack of situational awareness of events and	Senior leadership has limited situational awareness of DCIP remediation, mitigation, and reconstitution planning, response, and execution activities. Some DCIP community members appear to be unsure of their responsibilities and how to

ID	Current State	Gap
	response actions,	perform the business processes that support the program, and how those responsibilities relate to others in the community. The information flow paths *up the chain* are not defined sufficiently and exercised often enough to satisfy leadership's requirements without significant expenditure of resources at the time of an event. Leadership's information requirements are not well defined.
3.	Many DCIP community members are frustrated with the lack of recognition by their leadership about DCIP and the consequent difficulty in obtaining funding to support the program.	While publication of the DoDD 3020.40 and the Interim Implementation Guidance are critical elements to support budget advocacy, the future success of the program will be determined by the levels of funding that are obtained independently by the Service, Sector, and Agency DCIP representatives ASD (HD) DCIP needs to develop a strategy to assist DCIP community members in obtaining the funds needed, and to provide consulting-type services to help the community obtain finds for DCIP
4.	The nature of DCIP requires significant interaction and coordination among the Services, Sectors, and Agencies. This requirement is currently being addressed by the CIPIS and the DISC.	While the CIPIS and the DISC provide a loose structure dedicated to sharing program information and to addressing specific procedural and technical issues, implementation of the DCIP requires cross-community organizational structures that are more attuned to accomplishing the work of implementing the program. Additionally, a Community of Interest is required to provide context for the data sharing and metadata definitions required for registration in the Net-Centric Environment.
5.	Each member of the DCIP community defines its data according to its internal business needs and its understanding of DCIP information requirements.	The many definitions and interpretations of DCIP-related data often conflict at the data definition level and make seamless information sharing extremely difficult, time-consuming and costly.

ID	Current State	Gap
6.	With over 20 independent systems supporting DCIP business needs, the community has stovepiped information and data distributed across multiple systems. Information is shared via reports and data calls.	The DCIP mission requirements, as executed in a resource-constrained environment, require improved information sharing. The most effective means of satisfying this requirement is to leverage the Net-Centric GIG to the maximum extent possible.

7.2 Recommendations

The true value of an IEA is achieved only when it is implemented in a manner that satisfies its sponsor's business needs. The Transition Plan includes a series of Transition Initiatives that address implementation of the IEA to provide the levels of information sharing required for accomplishment of the DCIP mission. These Initiatives recognize that dramatic change needs to occur in incremental stages. Additionally, DCIP recognizes that a series of Transition IEAs will need to be constructed to guide implementation. This AV-1 recommends the following actions:

- Implement the Initiatives in the Transition Plan as soon as practical.
- Continue documenting business processes as the DCIP matures and evolves. Flow these changes into a series of evolving Transition IEAs.