The Department of Defense

Internet Protocol Version 6

Transition Plan

Version 2.0

June 2006

Assistant Secretary of Defense for Networks and Information Integration/
Department of Defense Chief Information Officer

The Department of Defense
Internet Protocol Version 6
Transition Plan

This plan (Version 2) updates the transition plan submitted to Congress in March 2005. It describes the overall strategy for IPv6 transition, identifies roles and responsibilities, and outlines transition governance, milestone objectives, and the foundation for more in-depth efforts. Additionally, the plan contains guidance on obtaining IPv6 capable products; tests and demonstrations; responsibilities for the transition of networks, applications, and infrastructure; criteria for demonstrating transition readiness; and the strategy for leveraging commercial IPv6 work. This plan will be updated as required.

Approved by: _____
for

John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Dated: June 30 2006

Table of Contents

List of Figures

1 Introduction

1.1 Overview

Internet Protocol Version 6 (IPv6) is the next-generation network layer protocol for the internet and the DoD Global Information Grid (GIG). As described in the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) June 9, 2003 memo[1], the achievement of Net-Centric Operations and Warfare (NCOW), envisioned as the GIG of inter-networked sensors, platforms, facilities, people and information, depends on effective implementation of IPv6 in concert with other aspects of the GIG architecture. In this architecture, the Internet Protocol (IP) is the common network protocol that allows all types of data to move seamlessly on the GIG's diverse transport layer which includes landline, radio, and space-based elements. Per the above memo, implementation of IPv6 is necessary due to fundamental limitations of the current Internet Protocol Version 4 (IPv4) protocol[2] for the long-term networking requirements of the DoD and commercial community. The June 9, 2003 memo directs a series of steps and activities to support that implementation, including developing a transition plan.

1.2 What is IPv6?

IPv6 is designed to support internet growth in number of users and functions. The current version, IPv4, was developed in the 1970s and is the basis of interoperability for today's internet and many DoD networks. However, IPv4 has limitations that may inhibit the end-to-end paradigm of the internet and achievement of DoD's vision of net-centric operations.

IPv6 has been under development by the internet community for over a decade and is designed to overcome these limitations by greatly expanding available IP address space and integrating features such as end-to-end security, mobile communications, Quality of Service (QoS), and simplified network management. Numerous "fixes" and extensions to IPv4 have been implemented to overcome these limitations. However, these have usually increased network complexity and slowed network performance. IPv6 will add functionality and reduce network complexity.

[1] ASD(NII)/DoD CIO Memo, Internet Protocol Version 6 (IPv6), June 9, 2003.
[2] Internet Engineering Task Force Request for Comment 1454, Comparison of Proposals for Next Version of IP, May 1993.

1.3 Why IPv6 Transition is Important to the DoD

IP is the foundation of interoperability across the DoD, enabling secure connection of people and systems, independent of time or location. Sensors, platforms, and weapons are built as "net-ready" nodes incorporating IP-based protocols.

IPv6 features facilitate achieving net-centric operations. The features of most importance to the DoD include:

- **Improved End-to-End Security.**
    - End-to-end packet security is a fundamental requirement for net-centric operations. IPv6 security features provide significant capabilities for authentication, data integrity, replay protection, and confidentiality. IPv6 includes additional security features such as mandatory Internet Protocol Security (IPSec) for all information flows. While IPSec can be used with IPv4, it is primarily used in a gateway mode for Virtual Private Networks (VPN) and remote access. When end hosts migrate to IPv6 implementations with mandatory IPSec, end-to-end security will enable services such as secure IP mobility and secure peer-to-peer communications.
- **Quality of Service Flexibility.**
    - QoS is increasingly important for networking environments to support real-time and near-real-time applications, including voice, conferencing, collaboration, and video. IPv6 contains an 8-bit, Traffic Class field, which, in conjunction with an added Flow Label field, will be able to better specify quality and policy-based networking capabilities. Advanced QoS features are not inherent in any IP header, but require capabilities in the router, other networking devices, and applications.
- **Improved Mobility.**
    - IPv6 provides significant advantages over IPv4 in mobility. The DoD has increasing demands for mobile computing power and networking infrastructure to support it.
- **Simplified Network Management.**
    - Managing IPv4-based networks is increasingly complex as fixes and patches are implemented to overcome limitations of IPv4. IPv6 can provide features such as address auto-configuration and neighbor discovery.

- **"Unlimited" Address Availability.**

    - The shortage of IPv4 addresses has been a primary driver in the development of IPv6 by the commercial and international community. While not a primary driver for near-term DoD adoption (which has about 18% of the world's available IPv4 addresses), the greatly expanded IPv6 address space provides an opportunity to redesign the DoD address space to better accommodate future proliferation of unmanned sensors and mobile assets. Address space is increased from 4.29×10^{9} unique addresses provided by IPv4 to 3.40×10^{38} IPv6 addresses.

As depicted in Figure 1-1, transition to IPv6 will affect the entire DoD IT infrastructure. Many of the new DoD capabilities being developed need to operate in an IPv6 world. The DoD has committed to a major investment in transforming the GIG and achieving net-centric operations. This includes programs such as Transformational Communications Satellite (TSAT), Defense Information Systems Network (DISN), Net-Centric Enterprise Services (NCES), Joint Tactical Radio System (JTRS), and Future Combat Systems (FCS).

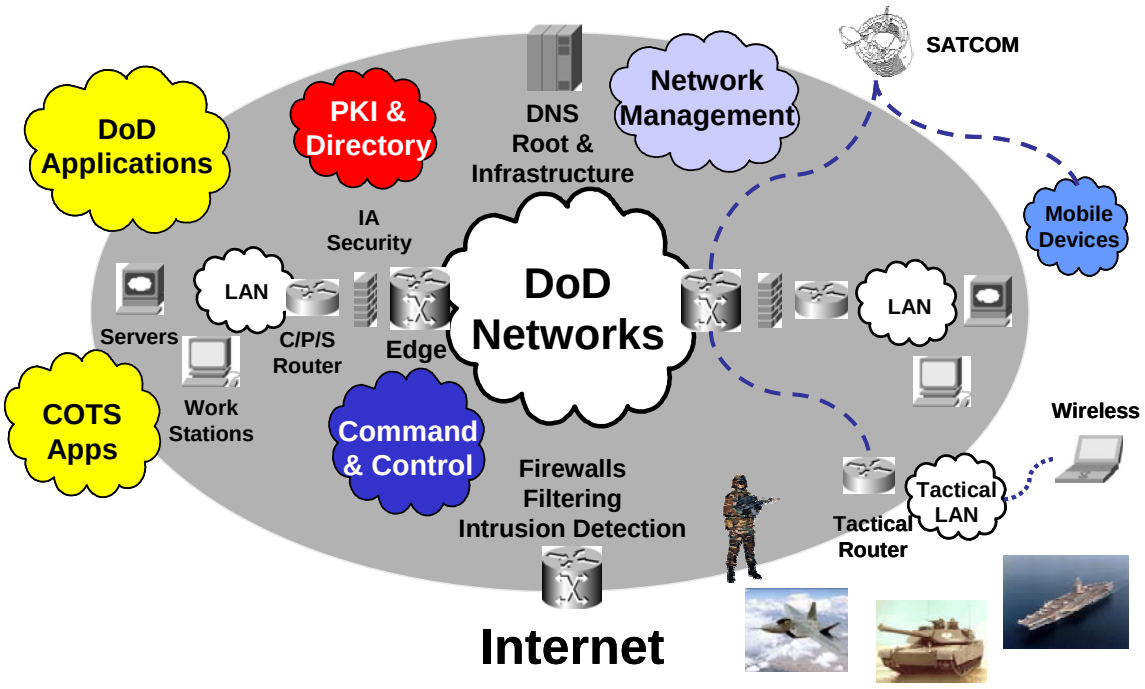

Figure 1-1 IPv6 Transition Implications

Transition to IPv6 is necessary for the DoD to avoid technological obsolescence. While the precise timing and speed of commercial deployments utilizing IPv6 are uncertain, it is expected to replace IPv4 over the next several years. Today there are global and technological pressures for the internet transition to IPv6. With the increasing proliferation of IP-addressable devices, including potentially billions of IP-enabled mobile devices, this problem is becoming more acute and the pressures for a transition are building. While most of the implementations are still in the research and engineering

communities, this is changing. Currently, some Internet Service Providers (ISPs) have started to offer commercial IPv6 service. The DoD is dependent upon Commercial Off-the-Shelf (COTS) products from hardware and software vendors. Many of the major vendors are now developing, or have committed to develop in the near-term, IP layer dual stack[3] products. While these dual stack products are planned to be available for the near-term, it is expected that these products will become IPv6-only.

1.4 DoD IPv6 Transition Plan

A number of actions were included in the ASD(NII)/DoD CIO June 9, 2003 memo to implement IPv6 for DoD networking in an integrated, secure, and effective manner:

- As of October 2003, all GIG assets being developed, procured or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems)
- Significant portions of the GIG will transition to IPv6 to build confidence for completing the transition
- Defense Information Systems Agency (DISA) shall acquire and manage IPv6 addresses for the DoD, including establishment of address and naming conventions
- IPv6 implementations will not be fielded on networks carrying operational traffic within DoD at this time (a temporary measure to ensure that security concerns during transition are addressed in the transition plan)
- An IPv6 transition plan will be developed.

The ASD(NII)/DoD CIO, in consultation with the Joint Staff and with the participation of DoD Components, was tasked to lead the development of the IPv6 transition plan. The transition to IPv6 is a complex issue with implications well beyond networks. IP and related protocols potentially touch almost everything from COTS and Government Off The Shelf (GOTS) applications to computer operating systems, network services (e.g., Domain Name Services), and core and distribution networks. IP is used across all DoD domains including Intelligence, Surveillance, Reconnaissance (ISR), and warfighting command and control, strategic, theater, and tactical operations.

[3] Support both IPv4 and IPv6 stacks.

In response to the June 9, 2003 memo, the ASD(NII)/DoD CIO, in conjunction with DoD Components, developed the DoD IPv6 Transition Plan, policy, and technical documentation (see Appendix B for reference documents) that address:

- Transition strategy and policy, including milestones and criteria for legacy, upgraded and new capabilities
- DoD IPv6 transition governance, and roles and responsibilities
- Acquisition and procurement of IPv6 capabilities
- Technical and test plans that support IPv4/IPv6 interoperability
- DoD IPv6 network, applications, and Information Assurance (IA) system transition approach and guidelines
- DoD IPv6 address planning and address space justification to the American Registry for Internet Numbers (ARIN)
- DoD IPv6 Master Test Plan (MTP) for Test and Evaluation (T&E) coordination
- IPv6 capable specification and DoD IT Standards Registry (DISR) Standard Profiles for IPv6 Capable Products
- IA requirements and guidelines for Certification and Accreditation (C&A) to field networks carrying IPv6 operational traffic
- Guidelines for early implementation of pilots
- Program manager, network engineer and application engineer guidebooks for DoD IPv6 transition managers and technical staff
- Milestone objective implementation guidelines
- Collaboration with industry.

1.5 Structure of the IPv6 Transition Plan

Figure 1-2 shows key elements of the work breakdown for a transition plan as well as the overall context. Three major aspects are considered: governance and outreach, risk reduction, and technical transition strategy including address space acquisition, architecture, and management.

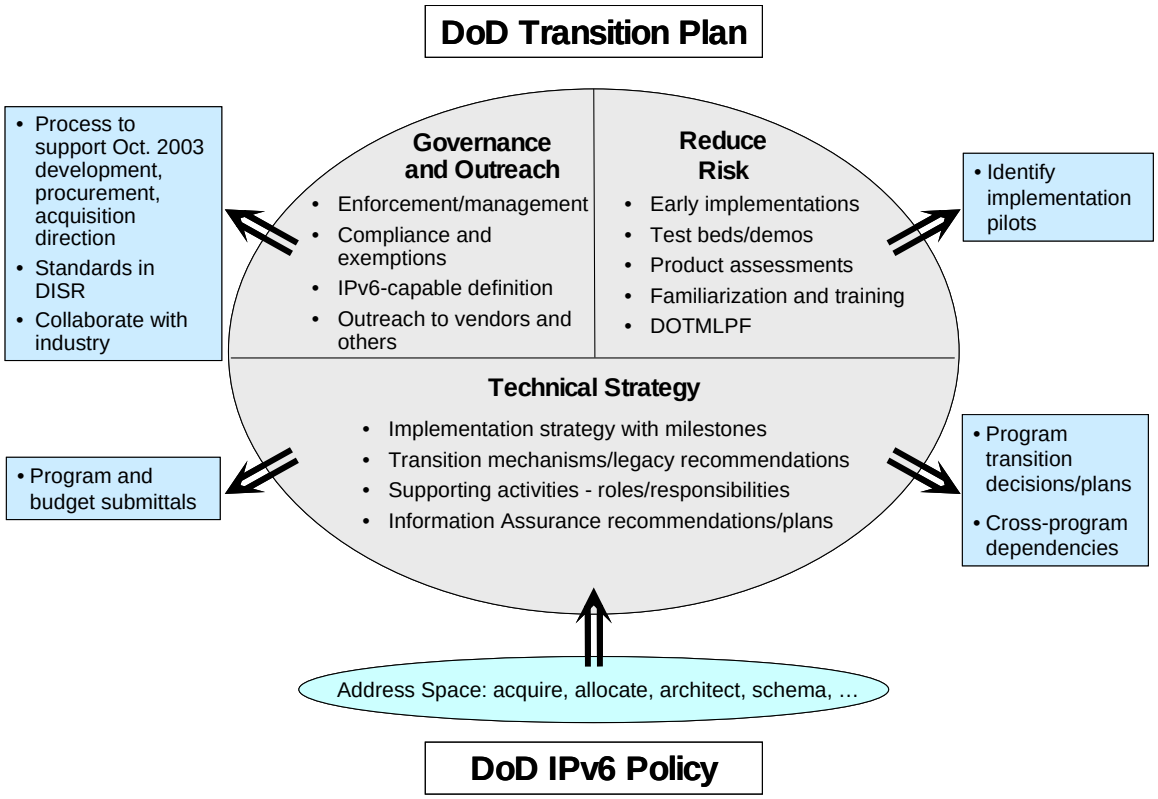

Figure 1-2 Key Near-Term DoD IPv6 Transition Activities

Governance is discussed in Chapter 2. Chapter 3 discusses key tenets of transition strategy. Chapter 4 deals with acquisition and procurement of IPv6 capabilities. Chapter 5 has the transition schedule. Chapter 6 discusses funding for transition. Appendix A discusses technical elements of transition, including plans to reduce risks through tests and demonstrations. Appendix B provides a list of IPv6 transition documents developed by the ASD(NII)/DoD CIO and the DoD IPv6 Transition Office (DITO).

2 IPv6 Transition Governance

2.1 Overview

Planning and executing DoD's transition to IPv6 requires close coordination and cooperation among all DoD Components. Ultimately, the transition will impact most Information Technology (IT), National Security Systems (NSS), and business applications and systems. To ensure that the Department's operational capabilities are not negatively impacted by IPv6 transition, the management structure, responsibilities, and processes are outlined in this section. As transition proceeds, the need for IPv6-focused entities will be annually reevaluated to determine if existing management structures and processes need to be modified.

This transition plan is based on an integrated and coordinated transition across DoD with distributed responsibilities. Coordination and integration of efforts is achieved through developing and maintaining coordinated and integrated tools such as transition plans, test plans and schedules; establishment of a DoD IPv6 Transition Office; and creation of a set of IPv6 working groups under the DoD CIO Executive Board to cooperatively address critical issues across the DoD on a continuing basis. The ASD(NII)/DoD CIO has overall responsibility for ensuring a coherent and timely transition to IPv6 across the DoD that ensures interoperability and security. DoD Components are responsible for executing the policies and guidance. Enforcement will generally be through existing budgetary and acquisition review processes. The following sections discuss the governance structure in more detail.

2.2 IPv6 Governance Structure

To effectively engage the DoD Components in transition planning and implementation, a management and technical structure involving DoD Components and addressing critical aspects of the transition in a long-term systematic approach has been implemented. Figure 2-1 illustrates the current governance structure for IPv6 transition.

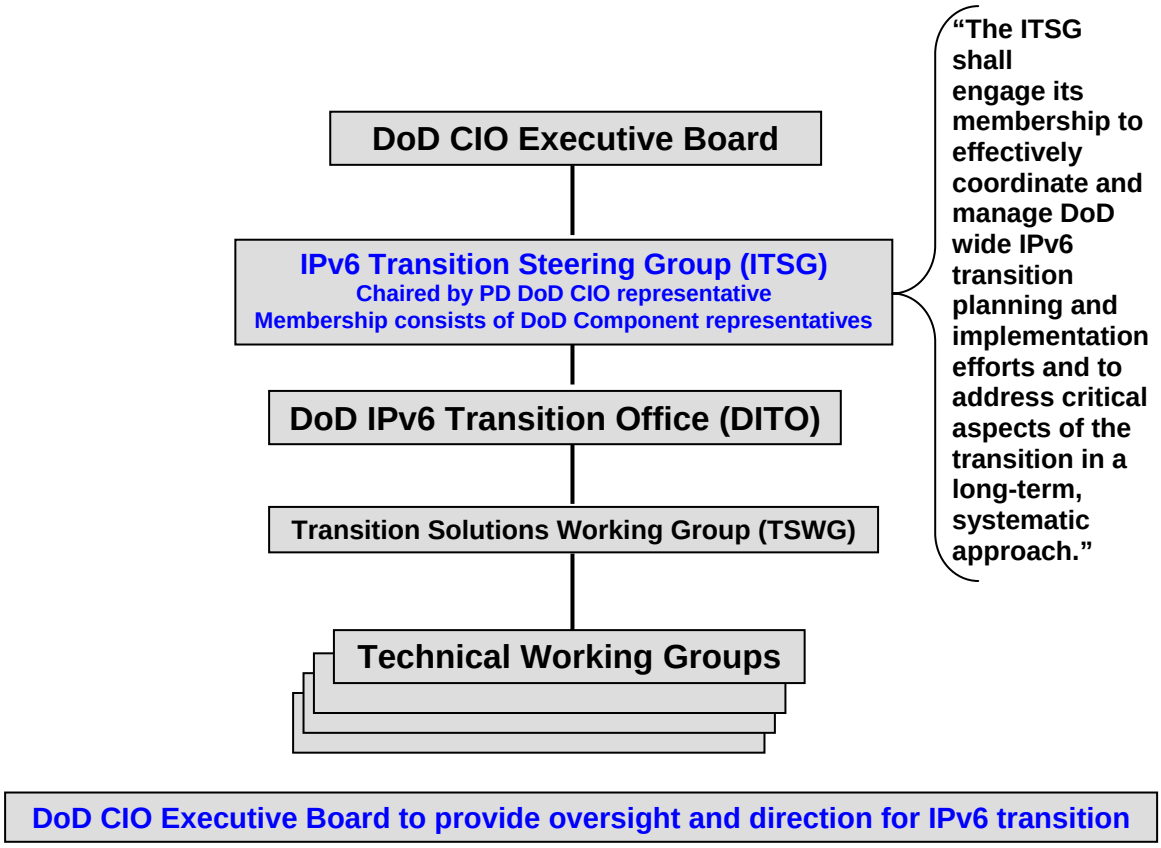

Figure 2-1 IPv6 Governance Structure

The DoD's IPv6 transition organization is a three-level structure consisting of the DoD CIO Executive Board, IPv6 Transition Steering Group (ITSG), and the DITO. The transition organization provides strategy, objectives, direction, and policy guidance.

The Principal Deputy DoD CIO and the DoD CIO Executive Board provide top level oversight and guidance to the ITSG. The ITSG provides a forum to coordinate policy and provide oversight and direction. The ITSG proposes, reviews, and coordinates IPv6 transition policies; reviews and coordinates IPv6 implementation schedules; reviews critical issues and defines associated strategies for addressing these issues. The ITSG charter derives its authority from and fulfills the requirements established in the DoD IPv6 Transition Plan and is signed by the DoD CIO Executive Board chair. The ITSG is chaired by a representative from the office of Director, Architecture and Interoperability, Principal Deputy DoD CIO. ITSG membership is open to representatives from all DoD Components. The CIO Executive Board is briefed periodically on IPv6 transition by the ITSG chair or his representative.

Major focus areas for the DoD CIO Executive Board and the ITSG include:

- Establishing, chartering, and dissolving working groups
- Overseeing and focusing DITO activities

- Addressing programmatic issues that affect IPv6 implementation
- Resolving issues brought forward by DoD Components
- Providing periodic updates to the DoD CIO Executive Board
- Planning for implementation and transition of IPv6
- Monitoring implementation progress and ensuring enterprise-wide consistency with common solutions
- Coordinating key IPv6 planning and implementation documents
- Addressing issues concerning interoperability, commonality, and standardization of IPv6.

The DITO provides guidance and addresses transition solutions and issues the DoD Components have in common, as described in section 2.3.10. The DITO is the secretariat for the ITSG; and the chair and secretariat for the Transition Solutions Working Group (TSWG).

The purpose of the TSWG is to provide a forum to coordinate technical solutions and guidance, resolve technical and programmatic issues, and provide oversight and direction across DoD Components in support of the transition. The TSWG charter is signed by the ITSG chair or his representative, and the TSWG receives its guidance from the ITSG. To address specific technical issues, the TSWG established subordinate technical working groups.

2.3 Roles and Responsibilities

The following subsections describe the roles and responsibilities of DoD Components involved in the DoD IPv6 transition. These are not intended to redefine, reallocate, or otherwise alter existing DoD Component roles and missions.

2.3.1 Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer

The Assistant Secretary of Defense for Networks and Information Integration/ Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) has overall responsibility for ensuring a coherent, timely transition to IPv6 across the DoD that ensures interoperability and security. To accomplish that responsibility, the ASD(NII)/DoD CIO issues guidance and policy as needed.

The ASD(NII)/DoD CIO is responsible for approving the DoD IPv6 Transition Plan and updates. The ASD(NII)/DoD CIO, in conjunction with Director, Operational Test &

Evaluation (DOT&E), approves the DoD IPv6 MTP. The ASD(NII)/DoD CIO and DOT&E are responsible for ensuring the Joint Staff IPv6 operational criteria (section 3.3) are successfully tested and demonstrated. The ASD(NII)/DoD CIO will also ensure that the required transition progress is being made. To the extent feasible, existing processes (such as acquisition reviews) will be used to ensure policy is being followed.

The ASD(NII)/DoD CIO will coordinate with DoD Component Acquisition Executives (CAEs) and Program Executive Offices (PEOs) on any joint, defense-wide, or Intelligence Community (IC) programmatic IPv6 issues.

The ASD(NII)/DoD CIO is responsible for ensuring end-to-end systems engineering initiatives support IPv6 transition efforts. Furthermore, the ASD(NII)/DoD CIO must ensure that efforts of the DITO, end-to-end system engineering, and net-centric enterprise services are harmonized and address highest-priority needs.

The DoD CIO chairs the DoD CIO Executive Board and oversees all IPv6 implementation activities including planning, funding, testing, acquisition, and other required activities such as coordinated outreach to vendors, standards bodies and other governments.

The Principal Deputy DoD CIO is responsible for day-to-day oversight and management of IPv6 transition planning and implementation.

2.3.2 Director, Operational Test & Evaluation

The Director, Operational Test & Evaluation (DOT&E), in conjunction with the ASD(NII)/DoD CIO, shall approve the IPv6 MTP. DOT&E, in conjunction with ASD(NII)/DoD CIO, is responsible for ensuring the Joint Staff IPv6 operational criteria (section 3.3) are successfully tested and demonstrated. DOT&E will provide guidance and input to the ASD(NII)/DoD CIO and DITO for IPv6 test strategy and activities and will assist in identifying appropriate test organizations and facilities across the DoD. DOT&E shall work with the ASD(NII)/DoD CIO, Joint Staff, and DITO to clearly define operational metrics to measure progress. DOT&E will observe IPv6 tests and provide independent assessments of progress to the ASD(NII)/DoD CIO and DITO. DOT&E shall participate in the ITSG and subordinate technical working groups.

2.3.3 DoD Components

DoD Components consist of the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense. DoD Component CIOs shall ensure that an IPv6 transition plan is developed that includes network transition strategies, transition activities, and timelines. DoD Component

transition plans will be considered annexes to the DoD IPv6 Transition Plan. The plans will be updated as needed and reflect progress made, as well as future plans. DoD Components shall ensure, in conjunction with the Director, National Security Agency (NSA), that IPv6 IA issues are identified and included in transition planning efforts.

DoD CAEs and CIOs are responsible for ensuring that all IT capabilities being acquired, procured or developed are IPv6 capable. DoD Components will provide the ASD(NII)/DoD CIO with copies of implementation guidance issued. DoD Component CIOs will coordinate with CAEs on IPv6 for DoD Component-specific programs.

DoD Component CIOs will ensure that IPv6 implementation requirements are included in budget and Program Objective Memorandum (POM), to include resources needed for testing, engineering, and pilot implementations, as well as overall transition of legacy IT.

Each DoD Component is responsible for the transition of respective IT assets. DoD Components must identify and develop solutions for operational requirements unique to the DoD Component (e.g., low-bandwidth operations and mobility). DoD Components shall identify, resource, engineer, and field pilot IPv6 implementations. These pilots should be operational segments of the GIG that will help build confidence for the DoD's complete transition.

DoD Components shall participate in the IPv6 governance structure (section 2.2) to ensure that an integrated IPv6 implementation is achieved across the DoD. Each DoD Component shall establish an IPv6 transition office to manage IPv6 transition within the DoD Component.

2.3.4 Chairman of the Joint Chiefs of Staff

The Chairman of the Joint Chiefs of Staff (CJCS) is responsible for ensuring that all new requirements for joint systems take into account operation in an IPv6 environment. The CJCS shall also ensure that IPv6 issues are addressed in planning documents and transition mechanisms are included as part of applicable capabilities documents. The Joint Capabilities Integration and Development System (JCIDS) process (CJCSI 3170.01E) shall ensure that the directed Initial Capabilities Document (ICD), Capabilities Development Document (CDD), Capabilities Production Document (CPD) and Integrated Architectures incorporate IPv6 capabilities as a requirement.

The CJCS shall certify that conversion of DoD networks to IPv6 will provide equivalent or better performance and capabilities than that which would be provided by any other combination of available technologies or protocols. Additionally, the CJCS has identified a set of DoD IPv6 operational criteria that must be successfully demonstrated before transition to IPv6.

The CJCS shall ensure that joint testing activities address IPv6 compatibility and interoperability on an end-to-end basis. The CJCS shall ensure, in conjunction with

NSA, that IPv6 IA issues are identified and included in transition planning efforts. The CJCS shall validate the DISA Joint Interoperability Test Command (JITC) IPv6 test results and interoperability certifications. The CJCS shall review NSA's Joint Service Cryptographic Modernization Implementation Plan for inclusion of IPv6 cryptographic equipment.

2.3.5 U.S. Joint Forces Command

As the joint force integrator, the U.S. Joint Forces Command (USJFCOM) shall represent and articulate the needs of the joint warfighter for IPv6 capabilities. USJFCOM shall also provide the operational impacts of using IPv6 and recommend T&E priorities.

2.3.6 National Security Agency

The National Security Agency (NSA) shall develop, in conjunction with DoD Components, IA guidelines to support implementation of IPv6 Milestone Objectives (MOs) (section 3.5). In addition, NSA has developed an IPv6 capable High Assurance Internet Protocol Encryptor (HAIPE) specification (version 3) required for IPv6 implementation on classified networks. NSA shall test and evaluate HAIPE functionality and performance characteristics, in conjunction with the DoD Components.

The NSA shall work closely with DoD Components in developing an IPv6 GIG End-to-End IA Architecture to ensure a timely, secure, and operationally-effective IPv6 environment. The NSA shall also develop the necessary Joint Service Cryptographic Modernization Implementation Plan.

2.3.7 Defense Intelligence Agency

The Defense Intelligence Agency (DIA) is responsible for planning and implementing the timely transition of the Joint Worldwide Intelligence Communication System (JWICS). DIA shall work with the DoD Intelligence Community Accreditation Support Team (DICAST) to certify JWICS IPv6 capabilities. This shall allow for accreditation of transition of the Secure Compartmentalized Information (SCI) portion of JWICS. DIA shall ensure, in conjunction with NSA, that IPv6 IA issues are identified and included in transition planning efforts.

2.3.8 Defense Information Systems Agency

The Defense Information Systems Agency (DISA) established the DoD IPv6 Transition Office to provide overall technical coordination, engineering, guidance, and assistance across the DoD to support an integrated and coherent transition.

DISA responsibilities shall include:

- Coordinating DoD's IPv6 standards with Industry, Internet Engineering Task Force (IETF), International Telecommunications Union (ITU), Institute of Electrical and Electronics Engineers (IEEE), and other standards bodies to ensure DoD needs are reflected in evolving IPv6 standards

- Acquiring, allocating and managing IPv6 address space for the DoD

- Providing top-level IPv6 Domain Name Service (DNS) support for the DoD, including internet root server(s)

- Conducting interoperability tests and certification for IPv6 products and capabilities

- Ensuring, in conjunction with NSA, that IPv6 IA issues are identified and included in transition planning efforts.

In addition to these DoD-wide responsibilities, DISA shall also be responsible for planning and implementing transition of DISN (Unclassified but Sensitive Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), Defense Switched Network (DSN), and Teleport) and NCES.

2.3.9 DISA Joint Interoperability Test Command

DISA JITC is an independent operational and test evaluation assessor of DISA, and other IT and NSS. DISA (JITC) provides joint and combined interoperability testing, evaluation and certification of IT and NSS. It also provides interoperability support, operational field assessment, and technical assistance to the DoD Components.

DISA (JITC) shall perform IPv6 performance and load testing, routing interoperability, and Multi-Protocol Label Switching (MPLS) interoperability tests. DISA (JITC) shall also perform IPv6 application and transition mechanism testing and evaluate end-to-end interoperability in mixed IPv4/IPv6 environments. DISA (JITC) shall develop and maintain an IPv6 vendor and DoD equipment, software, hardware and applications interoperability matrix and an Approved Products List (APL). DISA (JITC) shall also participate in DoD IPv6 working group meetings.

DISA (JITC) is responsible for testing and certifying IPv6 products. DISA (JITC) has developed the IPv6 Generic Test Plan (GTP), which is modular and scalable, to evaluate products using conformance, performance, and interoperability testing. The IPv6 GTP specifies test criteria and procedures for certifying IPv6 products. Products certified using the IPv6 GTP will be placed on the APL.

2.3.10 DoD IPv6 Transition Office

The DoD IPv6 Transition Office (DITO) shall ensure a coherent, timely transition across the DoD. This office is responsible for providing common engineering solutions and guidelines designed from an enterprise perspective. The DITO also has responsibility for coordinating transition planning, analyses, testing, and implementation efforts across the DoD, promoting knowledge-sharing, ensuring that needed infrastructure is provided, and implementing a systematic program of outreach within the DoD community. The DITO will ensure that critical transition issues are prioritized and addressed.

The DITO responsibilities for integrating and coordinating transition efforts shall include:

- Supporting and coordinating the updates of the DoD IPv6 Transition Plan and ensuring that DoD Component transition plans are synchronized and consistent
- Leading the development of more in-depth transition guidance and/or policies (e.g., implementation schedules)
- Leading (or supporting) DoD IPv6 working groups by providing technical and secretariat support
- Coordinating IPv6 efforts within the DoD
- Coordinating IPv6 issues with other federal agencies, North Atlantic Treaty Organization (NATO), coalition partners, and other entities
- Tracking IPv6 transition progress and providing assessments/recommendations to the ASD(NII)/DoD CIO
- Providing a department-wide IPv6 portal and knowledge base for information exchanges and outreach.

The DITO responsibilities for providing necessary infrastructure to support the transition shall include:

- Developing and updating an IPv6 addressing plan/architecture which considers enterprise needs, both near and long-term
- Ensuring that necessary IPv6 infrastructure is in place including DNS upgrades, root server(s), and Public Key Infrastructure (PKI) and Key Distribution Center (KDC) support.

The DITO responsibilities for ensuring that common solutions are used shall include:

- Ensuring that technical trade studies, assessments, and tests to address critical transition issues (e.g., transition mechanisms, DoD operational environment, network management, emerging standards) are performed

- Providing guidance and configuration recommendations for IPv6 network and IA implementation

- Supporting use of IPv6 capabilities (e.g., QoS, mobile networking, multicast, voice, video, security) by ensuring necessary research, analyses and planning are performed

- Providing IPv6 application transition and development guidelines based on best practices, DoD needs, assessments, and tests

- Conducting evaluations of IPv6-related research, technology, products, and commercial implementation

- Identifying IPv6 standards issues and influencing development of commercial standards and products that will satisfy DoD requirements

- Ensuring, in conjunction with NSA, that IPv6 IA issues are identified and included in transition planning efforts.

3 IPv6 Transition Strategy

3.1 Background

Today's DoD IP networking enterprise is a diverse environment serving hundreds of thousands of users with unclassified and classified core IPv4 networks. Edge networks include not only thousands of fixed-base distribution systems, but also large, low-bandwidth tactical network extensions to serve an increasing number of mobile users. Implementation of IPv6 will impact not only network routers, but network services such as domain name servers, IA devices, computer operating systems (including desktops, Web and other servers, and embedded devices) and many applications.

The IPv4 and IPv6 protocols are not interoperable. Transition mechanisms must be used to achieve interoperability. These transition mechanisms include dual IP stacks, tunnels, and translation. Some transition mechanisms may be used as stand-alone; some can (or must) be used in combinations; and some are not readily scalable to an enterprise. Furthermore, use of transition mechanisms may introduce IA vulnerabilities.

Transition from IPv4 to IPv6 must not noticeably impact the everyday business, tactical, and strategic operations of the DoD. Transition must be manageable, affordable, secure, and synchronized across all DoD Components. The entire transition process will likely span several years due to the scope, complexity, and cost involved.

As with any new technology insertion, schedule slips, security vulnerabilities, and unmet performance goals could occur. DoD Component transition offices and the DITO are performing risk analyses and adopting a risk mitigation process to avoid adverse effects. To ensure a smooth transition to an IPv6 environment and to minimize adverse effects, the DoD has taken a measured and controlled approach to fielding IPv6.

3.2 Key Tenets of DoD IPv6 Transition

IPv6 is an important enabler to achieve the end-to-end IP network vision that is the foundation of net-centric operations. IPv6 transition will be accomplished in a controlled, time-phased manner, taking advantage of ongoing commercial and government development and technology-refresh cycles to reduce costs. Limited capability pilots associated with MOs (section 3.5) will provide experience and lessons learned to users and network operators. The transition will be accomplished in an integrated manner that ensures interoperability, performance, and security by applying the following key transition tenets and subordinate elements:

- **The DoD IPv6 transition shall be managed in an integrated and coordinated manner.**

  - The DITO was established within DISA to integrate and coordinate DoD transition efforts, identify infrastructure to support transition, and ensure that common solutions are engineered for the DoD

  - Time-phased transition plans and technical guidance have been developed and maintained by the DITO that provide network, addressing, application, T&E, and IA solutions

  - An IPv6 governance structure was established that involves the ASD(NII)/DoD CIO, DoD Components, and DITO to address critical issues on a continuing basis.

- **IPv6 transition shall be accomplished primarily through technology-refresh cycles.**

  - DoD Components are responsible for programming and budgeting funds required for IPv6.

- **IT and NSS assets developed, procured, or acquired shall be IPv6 capable.**

  - To minimize IPv6 transition costs, all IT and NSS developed, procured, or acquired since October 2003 shall be IPv6 capable.

- **IPv4/IPv6 interoperability shall be maintained throughout the transition.**

  - The DoD IPv6 MTP discusses the strategy and process for maintaining IPv4/IPv6 interoperability and IA certification

  - DISA (JITC) will perform IPv4/IPv6 interoperability test and certification

  - The DISR identifies standards for facilitating IPv4/IPv6 interoperability.

- **Demonstrate Joint Staff IPv6 operational criteria.**

  - The DoD IPv6 MTP decomposes the operational criteria and identifies roles and responsibilities for T&E of these criteria.

- **Turn on IPv6 capabilities in a carefully controlled manner.**

  - MOs (section 3.5) have been established which define timelines for authorization of use of IPv6 in enclave, cooperative multi-domain environments, and enterprise-wide deployment

- Milestone Objective 1 (MO1) authorizes use of IPv6 systems within an enclave environment as of October 2005

- Pilots authorized under MO1 (including selected networks, network services, and applications) will provide the DoD with the experience and lessons learned for transition.

- **Leverage commercial/industry standards and products.**

  - DoD is working IPv6 standards with industry, IETF, ITU, IEEE and other standards bodies to ensure DoD needs are reflected in evolving IPv6 standards.

3.3 Joint Staff IPv6 Operational Criteria

The following IPv6 operational criteria have been identified by the Joint Staff. These criteria identify the key operational and technical issues that must be successfully demonstrated for IPv6 transition. The Joint Staff IPv6 operational criteria are:

- Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of High Assurance IP Encryptors (HAIPE), integration of IPSec, and integration with firewalls and intrusion detection systems

- Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment

- Demonstrate equivalent to, or better performance than, IPv4 based networks

- Demonstrate voice, data, and video integration

- Demonstrate effective operation in low-bandwidth environments

- Demonstrate scalability of IPv6 networks

- Demonstrate support for mobile terminals (voice, data and video)

- Demonstrate transition techniques

- Demonstrate ability to provide network management of networks

- Demonstrate tactical deployability and ad hoc networking.

The Joint Staff IPv6 operational criteria have been further decomposed into testable or verifiable measures of performance. Details can be found in the DoD IPv6 MTP (version 2).

Additionally, the CJCS shall certify that conversion of DoD networks to IPv6 will provide equivalent or better performance and capabilities than that which would be provided by any other combination of available technologies or protocols.

3.4 Critical Support Activities for IPv6 Transition

- **Acquisition of sufficient IPv6 address space for the DoD by DISA.**
    - DISA has provided justification for DoD IPv6 address space, which has been approved by the ARIN.
- **Management of overall IPv6 address space.**
    - DISA, in coordination with DoD Components, is developing a DoD IPv6 addressing plan that includes address-space and naming convention schema.
- **Ensuring Information Assurance needs are met.**
    - The DITO, in conjunction with NSA and the DoD IPv6 IA working group, has developed a DoD IPv6 C&A package consisting of IA risk management, IA C&A process, IA policy, and IA requirements documents. These documents provide the framework to help DoD managers perform security-risk management of IPv6 deployments to achieve Authority to Operate (ATO).
- **Program manager, network engineer, and application engineer guidance.**
    - The DITO has developed DoD IPv6 program manager, network engineer, and application engineer guidebooks to assist in the transition to IPv6. The purpose of these documents is to provide an understanding of the fundamentals of IPv6, its deployment, and strategies for managing the transition.

3.5 Initial IPv6 Implementation Phases

DoD policy requires potential security vulnerabilities to be understood and risks mitigated before IPv6 is allowed on networks that carry operational traffic. In conformance with this policy, the ASD(NII)/DoD CIO established a strategy to introduce IPv6 in a step-wise approach as IA risks are mitigated and issues are resolved. MOs have been established to provide a controlled transition to IPv6. This milestone objective approach first authorizes use of IPv6 in an enclave environment, then authorizes use of IPv6 across cooperative domain boundaries, and finally, authorizes IPv6 implementations enterprise-wide.

MO1 represents the first milestone objective in the DoD IPv6 transition, and the first instance that IPv6 traffic is authorized in enclave environments as of October 1, 2005.

The primary objective of the MO1 is risk mitigation, while permitting IPv6 use to demonstrate functional capability and build expertise for a DoD-wide transition. MO1 will leverage the existing knowledge base, qualified personnel, operations policies, and established standard operating procedures.

MOs are not a mandate, but an authority to implement and operate IPv6. The triggering events for authorizing each MO are the availability of IA implementation guidance and issuance of policy by the ASD(NII)/DoD CIO. It is the DoD Components decision to implement respective milestones, once authorized by the ASD(NII)/DoD CIO. Each IPv6 implementation must also complete the IA C&A process to achieve authority to operate.

Definitions of the MOs are provided below:

- **Milestone Objective 1 (MO1)**

  - DoD Components are authorized to implement and operate IPv6 within an enclave. At MO1, the evaluation of the IPv6 protocol is sufficient, and the policy, procedures, and technical guidance have been developed to authorize DoD Components to operate in a single network domain or enclave environment within operational networks. The single domain or enclave requires strict access controls be maintained under a single administrative authority for IA and security policy. Information flow will be tightly controlled to prevent IPv6 packets from entering or leaving the domain. The border device shall not translate nor permit the transit of native or tunneled IPv6 packets. MO1 allows the use, familiarization, and testing of IPv6 protocol and applications to ascertain issues and derive migration strategies for this new protocol. **MO1 was authorized as of October 1, 2005.**

- **Milestone Objective 2 (MO2)**

  - DoD Components are authorized to implement and operate IPv6 across cooperative domain boundaries. At MO2, the policies, procedures, and technical guidance have been developed to expand the operation of IPv6 across cooperative domain boundaries, but limited to within DoD networks (no internet exchange of IPv6 packets, native or tunneled). MO2 will provide the ability to evaluate the scalability and further evaluate the IPv6 IA implications using tunneling and native IPv6 routing, as available. IPv6 traffic which crosses cooperative domain boundaries must be approved in accordance with the DISN connection-approval process to ensure compliance with IA policies. Multiple certification and accreditation authorities may be involved in MO2. MO2 permits applications to test IPv6-specific end-to-end capabilities and routing schema efficiencies. Limiting operation to within DoD, and only at approved locations, reduces risk to IA and operational impacts on existing IPv4 networks. **Target date for MO2 is October 1, 2006.**

- **Milestone Objective 3 (MO3)**

  - DoD Components are authorized to implement and operate IPv6 enterprise-wide. At MO3, the policy, planning, and technical transition guidance will be provided to allow tunneled and native IPv6 traffic to exist on DoD operational networks. DISN and DoD Component core IP infrastructures are authorized to accept, route, and process IPv6 protocol traffic while maintaining interoperability with IPv4. Boundary protection, deep packet inspection, and other security mechanisms to assure IA requirements shall be available and implemented to protect the DISN. MO3 permits applications and data owners to complete operational transition to IPv6 with at least the same functionality (parity) as currently found in IPv4. **Target date for MO3 is Fiscal Year (FY) 2008.**

- **Future Milestone Objectives**

  - Future MOs shall be defined, as required, to represent achievement of specific IPv6 advanced features. These dates will be event and technology driven based on the maturing nature of the protocol. DoD Component transition offices shall identify specific advanced features to support the deployment of future systems.

3.6 IPv6 Documentation

The DoD IPv6 Transition Plan addresses the essential programmatic and technical aspects of IPv6 implementation. The DoD IPv6 Transition Plan will be updated annually. DoD Components shall participate in plan update reviews and provide comments. Updates shall address changes in the transition planning, as well as increased depth of coverage.

DoD Components shall also develop IPv6 transition plans. These DoD Component transition plans shall be consistent with the overall DoD IPv6 Transition Plan, but will focus on the transition within the respective DoD Component. The plan will include an implementation schedule for key networks and programs, as well as identification of DoD Component-specific issues and how they will be addressed. Critical dependency issues will be identified and worked through the ITSG.

Master plans shall be developed to facilitate IPv6 transition. These master plans shall include an IPv6 MTP, IPv6 Master Address Plan, IPv6 Master IA Plan, and IPv6 Master Implementation Plan.

A DoD IPv6 MTP has been developed in coordination with the ASD(NII)/DoD CIO, DOT&E, CJCS, DoD Components, and the DITO. The MTP defines overall IPv6 T&E strategies, identifies organizations responsible for executing the strategy, and identifies challenges that may impede IPv6 implementation. The MTP also identifies key IPv6

issues to be resolved through testing[4] and the strategy for addressing those issues, using distributed IPv6 laboratory testing, joint exercises, and acquisition testing. The intent of the plan is to coordinate IPv6-related T&E activities and consolidate test results to evaluate whether the Joint Staff IPv6 operational criteria have been demonstrated.

Detailed technical implementation guidance is required for IPv6 transition. To date, the DITO has developed DoD IPv6 program manager, network engineer, and application engineer guidebooks, and IA guidance for MO1 to assist in the transition to IPv6. Implementation guidance for subsequent MOs and an IA guidebook are in development. The purpose of this guidance is to provide an understanding of the technical fundamentals of IPv6, its deployment, and strategies for managing the transition.

Figure 3-1 shows the key IPv6 documentation to be used to facilitate DoD IPv6 transition.

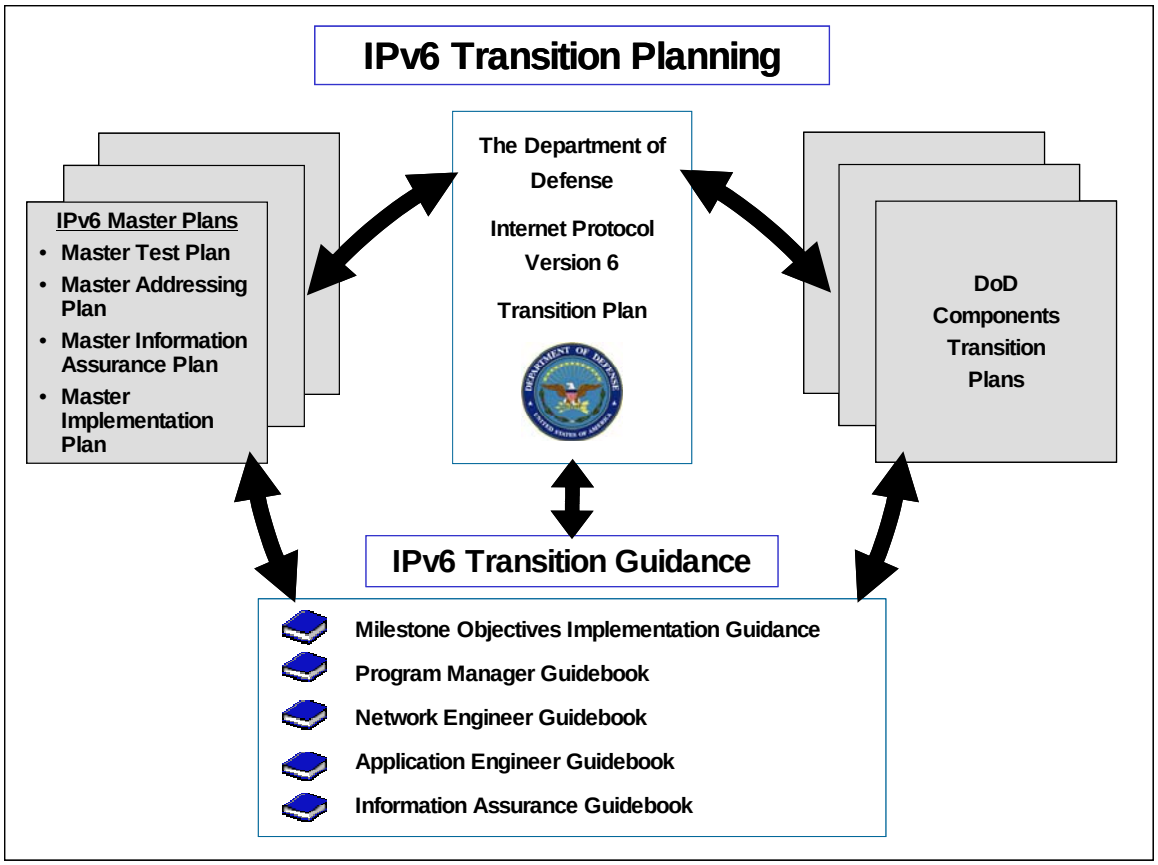

Figure 3-1 IPv6 Transition Planning and Guidance Documents

[4] Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System, May 12, 2003.

4 Development, Procurement, and Acquisition of IPv6 Systems and Products

4.1 Policy Framework

A key tenet of the DoD IPv6 transition strategy is to minimize transition costs by ensuring that COTS and GOTS products and systems developed, procured, or acquired after October 1, 2003, shall be IPv6 capable. The scope of systems and capabilities impacted by this requirement extends beyond routers (which handle and route IP packets). IP applications and security products (e.g., firewalls, intrusion-detection systems, packet encryptors) shall also be IPv6 capable.

4.2 Definition of IPv6 Capable

An IPv6 capable system or product shall be capable (once IPv6 enabled) of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4.

Specific criteria to be considered IPv6 capable are:

- Conformance with the DISR IPv6 Standard Profiles for IPv6 Capable Products
- Maintaining interoperability in heterogeneous environments and with IPv4
- Commitment to upgrade as the IPv6 standard evolves
- Availability of contractor/vendor IPv6 technical support.

4.3 IPv6 Capable Product Availability

Key software and hardware COTS vendors are committed to producing dual stack-capable products (IPv6 and IPv4). In many infrastructure areas, IPv6 capable COTS products are available. For example, most new operating systems incorporate dual IP stacks and most new router products incorporate IPv6. However, in other areas, IPv6 capable products are not currently available. For example, IPv6 capable IA and network management products are just starting to emerge. Major application vendors are currently developing IPv6 capable products.

4.4 Certification of IPv6 Capable Products

The DISR IPv6 Standard Profiles for IPv6 Capable Products delineate requirements for six product categories (hosts, network appliances, routers, layer 3 switches, information assurance devices, and servers). The need for additional categories, such as IPv6 application products, is being evaluated. The DoD will test IPv6 product implementations using interoperability and performance procedures documented in the IPv6 GTP. The GTP includes test scripts to evaluate: core IP functionality; routing and switching; transition mechanisms; common network applications; information assurance; mobility; quality of service; multicasting; and network operations and maintenance. Certified products will be placed on the APL. Further details on certification of IPv6 products may be found in the DoD IPv6 MTP.

4.5 Waivers

For systems and products which do not meet the IPv6 capable requirement stated above, DoD Component CIOs may waive the requirement for IPv6 capability based on consideration of operational need or business case, including long-term resource implications across the enterprise. The DoD CIO must be notified of any waivers granted and provided with the rationale 10 days prior to the effective waiver for final approval purposes.

IPv6 waivers are not required by DoD CIO policy for program implementations that do not meet the FY 2008 transition goal. DoD Components may establish policy requirements for IPv6 implementation schedules. DoD Components are requested to inform the DoD CIO of respective policies in this regard for information purposes only.

5 DoD IPv6 Transition Schedule

5.1 Background

The ASD(NII)/DoD CIO June 9, 2003 memo established a goal to transition DoD network systems to IPv6 by FY 2008. In the August 2, 2005 memo "Transition Planning for Internet Protocol Version 6 (IPv6)," the Office of Management and Budget (OMB) set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure.

The DITO is coordinating with DoD Components to develop a DoD-wide, consolidated IPv6 implementation schedule for major DoD networks and programs. This schedule will include specific system IPv6 transition milestones as well as the schedule for accomplishing critical supporting tasks. The DoD Components will update and maintain internal schedules (as part of the DoD Component IPv6 Transition Plan) on a continual basis. The implementation schedule will define activities that can be accomplished by the FY 2008 time frame and identify programs and networks transitioning beyond the FY 2008 goal.

The planning emphasis for FY 2008 has been on transitioning the core DoD network infrastructure. As such, the IPv6 implementation schedules for major DISA networks are presented in this section.

5.2 DISA IPv6 Implementation Schedule

DISA has developed IPv6 implementation schedules for NIPRNet, SIPRNet, and Teleport. IPv6 services will be the basic IP services currently available in the DISA networks listed. The networks will accept, route, and process IPv6 traffic while also providing IPv4 services. Advanced IPv6 features will be addressed post FY 2008.

Figures 5-1 through 5-3 show the DISA networks IPv6 implementation schedules. By the end of the third quarter FY 2008, NIPRNet provided edge routers will be dual-stacked to support both IPv4 and IPv6 routing and packet forwarding. To avoid unnecessary cost, the NIPRNet Hub/Access routers will be dual-stacked as customers attached to the hub routers request IPv6 services. The classified IPv6 SIPRNet services are scheduled to be available by July 2010 and the unclassified IPv6 Teleport services are targeted for July 2008. SIPRNet IPv6 service in FY 2010 assumes IPv6 capable HAIPEs will be available in sufficient quantity by the end of FY 2009.

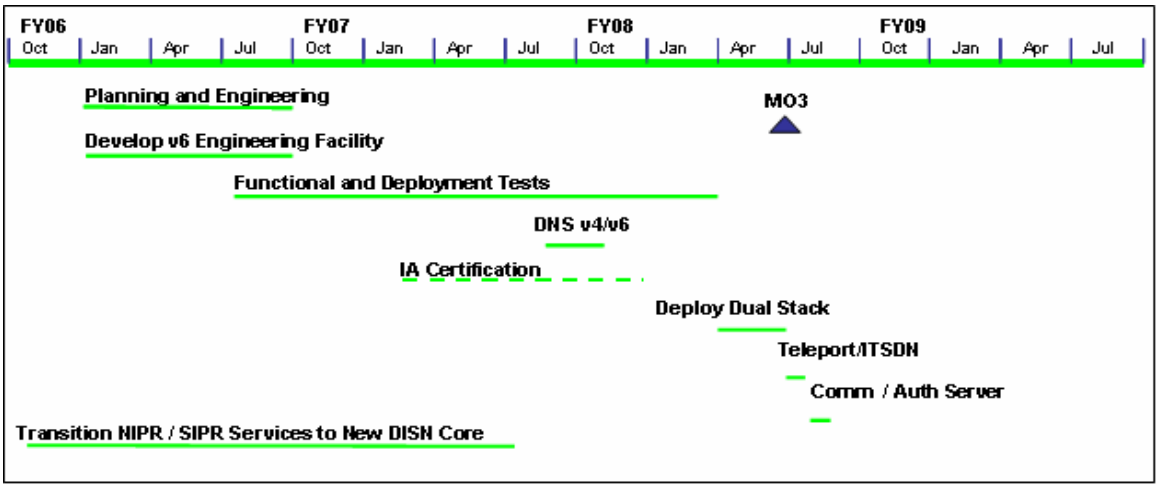

Figure 5-1 Schedule for DISN NIPRNet

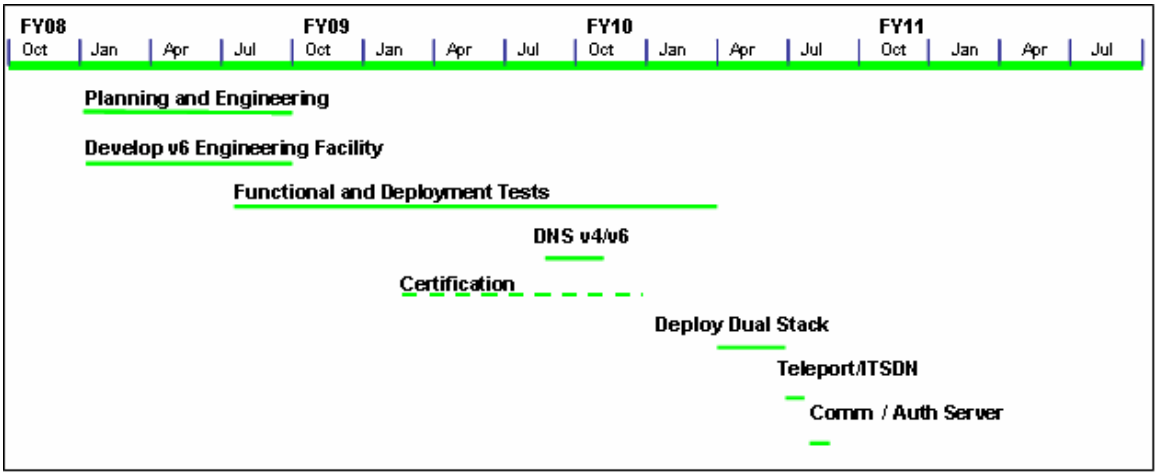

Figure 5-2 Schedule for DISN SIPRNet

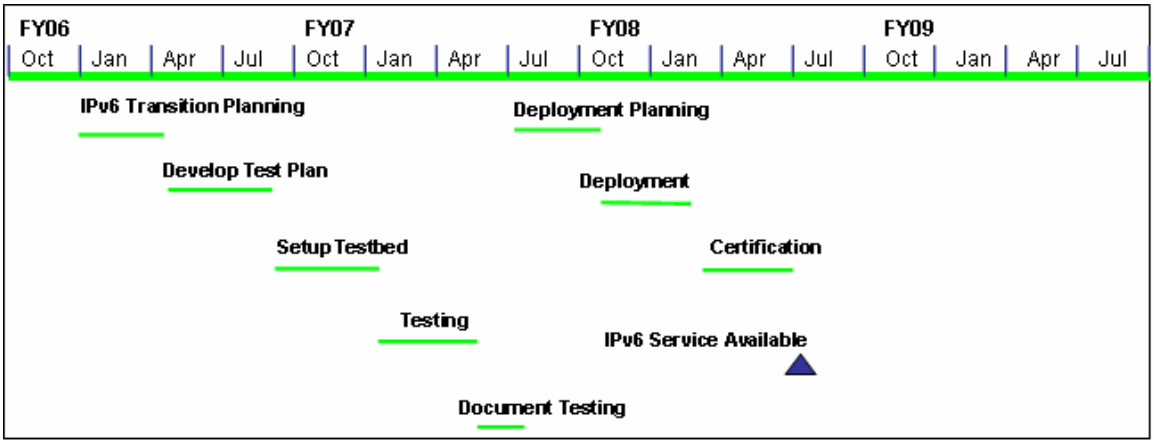

Figure 5-3 Schedule for DISN Teleport

5.3 DoD Components IPv6 Implementation Schedules

As part of wider DoD transition planning, the ASD(NII)/DoD CIO is working with DoD Component IPv6 transition offices to develop IPv6 implementation schedules for networks and programs that will transition by FY 2008 and those transitioning beyond the FY 2008 goal. The DITO will consolidate these schedules into an integrated DoD-wide IPv6 transition schedule.

6 Funding IPv6 Transition

The DoD's IPv6 transition strategy is designed to manage overall cost through incremental technology-refreshment and manage the risks associated with the DoD transition to IPv6. By starting to procure IPv6 capability on October 1, 2003, the DoD is building an inventory of the assets that are ready to operate with IPv6. In addition, by building IPv6 into the major next generation transformational capabilities being developed now and in the future, the DoD will avoid later transitional costs when these systems become operational. This strategy also allows the DoD to leverage ongoing commercial and industrial IPv6 work to better meet DoD needs.

Even with this strategy, there will be additional costs for this major technology transition to occur in a manner that protects enterprise interoperability, security, and performance. These additional costs are expected to be in the areas of:

- Planning, engineering, technical assessments, and training to support a coherent IPv6 transition
- Pilot IPv6 implementations and test beds necessary to minimize transition risks and demonstrate transition readiness, including necessary infrastructure
- IPv6 modifications to current development efforts
- Selective equipment and/or software replacements/modifications where timely technology-refreshments are not programmed.

The DoD Component IPv6 transition offices will minimize the additional cost by harmonizing enterprise transition efforts such as developing common engineering solutions, sharing knowledge, and avoiding duplicative testing and demonstrations. The DITO is responsible for providing overall technical assistance, performing engineering analyses of critical DoD issues, coordinating DoD-wide IPv6 transition planning and working group efforts, integrating IPv6 tests and demonstrations, and tracking implementation progress.

The POM process offers the DoD Components and the DITO (through DISA) the opportunity to fund the IPv6 transition requirements in the out years. However, this is expected to be challenging, given other DoD Component priorities, as well as the evolving understanding of the resources required. The availability of "new" funds to support IPv6 transition is not expected. DoD Components will have to rely on the refocusing of existing technology (and technology-refreshment) funds for the transition.

Appendix A: IPv6 Transition Elements

A.1 Overview

This appendix focuses on the key technical and operational issues, activities, and milestones required to transition to IPv6 across the DoD in a manner that protects interoperability, security, and performance. The applicability and scalability of these transition elements must be assessed and demonstrated.

The following sections of this appendix identify the activities required and progress made to accomplish the transition in terms of the network and infrastructure, IPv6 addressing, information assurance, tests and demonstrations, standards, applications, and training.

A.2 Networking and Infrastructure

The DoD's Wide Area Networks (WANs) infrastructure consists of a number of global IPv4 intranets which support the DoD's business, tactical, and strategic operations on an enterprise basis. These WANs interface with a diverse set of "edge" IP distribution networks that include thousands of fixed base/campus area networks, as well as, large tactical network extensions with generally low bandwidth connectivity and a dynamic environment including network access nodes and users that are mobile and/or transportable.

Careful planning will ensure that the DoD transition to IPv6 optimizes end-to-end performance, interoperability, security, scalability, and reliability. The network transition design must consider core and edge network transitions, and also the infrastructure (such as IPv6 addressing and Domain Name Services), information assurance and requirements, host transition schedules, and software applications. The IPv6 transition shall not disrupt everyday business, tactical, and strategic operations of the DoD. The complex task of transitioning these new and evolving legacy networks to IPv6 while maintaining the necessary security, performance, and interoperability cannot be underestimated. The issues to be addressed during transition include:

- Maintaining end-to-end network and application interoperability during the transition
- Ensuring that no additional security vulnerabilities are introduced by transition mechanisms used
- Exploiting the features of IPv6 (e.g., QoS) in a timely way that does not impact security or interoperability
- Developing an implementation plan that protects network performance and is aligned with already planned technology-refreshment schedules.

Although IPv6 is not backward compatible with IPv4, there are numerous transition mechanisms available (or emerging) to allow these two protocols to interoperate during the transition. These mechanisms generally fall into one of four broad categories:

- Dual Stack: a technique for providing complete support for both internet protocols, IPv4 and IPv6, in hosts, servers, and routers

- Configured tunneling of IPv6 over IPv4: point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures

- Automatic tunneling of IPv6 over IPv4: a mechanism for using IPv4-compatible addresses to automatically tunnel IPv6 packets over IPv4 networks

- Translation: a translator, located either as a "bump in the stack" middleware program or as a "bump in the wire" acts as a network translation gateway between IP nodes and converts IPv6 packets to IPv4, or vice versa.

Every mechanism proposed has potential implications in terms of performance, cost, scalability, and security. The DoD is evaluating these transition mechanisms in the context of overall DoD requirements and capabilities.

The DNS is an important network service that must also be available to support IPv6 transition. However, there are other important network services that may be impacted by the IPv6 transition, such as network time services, network management, and PKI. These impacts must be identified and any needed changes must be addressed.

A time-phased, end-to-end, DoD IPv6 network implementation plan (incorporating IA) is being developed by the DITO in coordination with DoD Components (including DISA and NSA). This will provide the framework for end-to-end IPv6 implementation across DoD networks and will be updated periodically. The DITO has developed an IPv6 Network Engineer Guidebook for assisting DoD Components in planning and implementing network infrastructure transition to IPv6.

A.3 Addressing

The ASD(NII)/DoD CIO June 9, 2003 memo tasked DISA to acquire enough IPv6 address space to meet DoD's five-year estimated requirements and initiate acquisition of IPv6 addresses to meet all future DoD requirements. DISA is also tasked to continue managing DoD IP address space (both IPv4 and IPv6) allocation, registration, and control on an enterprise basis to promote interoperability and security.

DoD's large allocation of IPv6 addresses, along with the inherent increased flexibility of having a large address space, will provide significant opportunities and challenges for DoD that need to be considered in the address plan. For example, wherever possible, DoD IPv6 address space should be distributed in a hierarchical manner, according to the

topology of the network infrastructure. This is necessary to permit the aggregation of routing information, limit the expansion of routing tables, and minimize router processing due to dynamic routing protocols.

A DoD IPv6 addressing architecture will be significantly different from today's IPv4 addressing architecture. For example, some DoD organizations with private intranets currently use Network Address Translation (NAT). In almost all cases, a NAT will not be needed with IPv6. Since all IP communications are directly dependent on addressing, and during the transition period both IPv4 and IPv6 addresses will be needed, unanticipated problems may arise when IPv4 and IPv6 are used simultaneously within the same infrastructure.

An interim DoD IPv6 addressing plan is being developed by the DITO to address near-term addressing needs of the DoD. Work is also proceeding on developing a long-term addressing plan and architecture for the DoD. The DITO is working with DoD Components in developing the long-term DoD addressing plan. This plan will provide for a global DoD presence and ultimately permit dynamic addressing for mobile forces and ad hoc networking. In developing this long-term plan, a hierarchical IPv6 addressing architecture and address allocation scheme that optimizes joint end-to-end performance, interoperability, and scalability is being developed which includes the allocation of space in a global, geographical, or geospatial manner. Force structure and deployment models will be needed to identify future requirements and the best addressing approaches.

Both the interim and long-term address plan will be compliant with current ARIN IPv6 address allocation and assignment policy. An assessment must be performed to determine ways to minimize any problems with fielding IPv4 and IPv6 addresses simultaneously within networks. Results will be incorporated into the IPv6 address plan as well as the DoD IPv6 network and IA system transition design.

In addition, DISA and Component Network Information Center (NIC) processes, procedures, policies, and databases must be upgraded to support transition. In particular, DISA will ensure that address management capabilities are adequate in terms of accuracy, response time and customer support.

A.4 Information Assurance

The ASD(NII)/DoD CIO June 9, 2003 memo directed an aggressive approach regarding the DoD implementation of IPv6. However, the memo recognized that there are security issues that need to be addressed before IPv6 can be used on DoD networks carrying operations traffic. Thus, for the transition to move forward, it is essential that IA issues be addressed and resolved on a progressive basis.

To address these security issues, the following needs to be accomplished:

- Development and assessment of recommendations regarding near-term use of IPv6 on DoD's networks that carry operations traffic, without increasing security risks
- Development and assessment of recommendations supporting the use of advanced features of IPv6 on DoD networks
- Provision of IPv6 capable HAIPE devices
- Assessments of proposed IPv6/IPv4 transition mechanisms and development of an integrated DoD IPv6 network and IA system transition design
- Configuration recommendations for IPv6 capable security devices (e.g., firewalls)
- Examination/participation in ongoing IETF IPv6-related standards work that has an impact on security/IA
- Assurance of the availability of IPv6 capable IA products, through the National Information Assurance Partnership (NIAP) process, including IPv6 protection profiles
- Consideration of all IPv6-related architectural issues as part of the GIG end-to-end IA Architecture Component.

Working with NSA and the IA working group, the DITO has developed an IPv6 C&A package that includes: IA policy, IA requirements, and IA risk management. The DITO has also developed a series of MO IA guidance documents.

A.5 Tests and Demonstrations

To meet the goal of completing the DoD IPv6 transition with acceptable risk requires a coordinated program of distributed test beds, pilots and field demonstrations, technical analyses, and modeling and simulation to address the key transition objectives of demonstrating the functionality of IPv6 as delineated in the Joint Staff IPv6 operational criteria.

The IPv6 T&E will be carried out in phases based on the MOs designed to mitigate risks in IA, performance, and interoperability. Early testing will emphasize IPv6 products, DoD IPv6 networks, and legacy applications.

The ASD(NII)/DoD CIO, in coordination with the DOT&E and other DoD Components, has developed an IPv6 MTP that will be updated periodically. The Test Plan is used to guide and manage the integrated IPv6 T&E program. The MTP describes the methodology and means for demonstration and verification of the Joint Staff IPv6 operational criteria. The MTP is intended to coordinate all IPv6-related testing activities across the DoD and consolidate test results to evaluate satisfaction of the Joint Staff IPv6 operational criteria and to plan subsequent IPv6 tests. The MTP also describes IPv6 product certification testing that will be conducted to populate an Approved Product List.

Pilot IPv6 implementations are needed to identify lessons learned and apply the resulting recommendations to other systems as they transition to IPv6. IPv6 pilot implementations will enable the DoD to move from experimental network environments, with a limited set of applications, through networks with a broader set of applications to enterprise-wide networks and a full representative suite of enterprise applications. DoD Components have been requested to nominate IPv6 pilots. Pilot nomination guidance has been issued to DoD Components in the Deputy CIO memo of August 16, 2005. The first network pilot for IPv6 testing was the Defense Research and Engineering Network (DREN). DREN IPv6 testing provided valuable lessons learned, such as that IPv6 performance was approximately the same as IPv4 on various stress tests and that security was comparable to IPv4 for WAN and site protection.

DISA has selected the Global Broadcast System (GBS) network for pilot testing and demonstration. The Navy is considering the Automated Digital Network System (ADNS) as an IPv6 pilot.

A.6 Applications[5]

Transition of DoD networks to IPv6 will be of limited value until applications and hosts that use IP networks are IPv6-enabled. The process for identifying, modifying, testing, and certifying this large number of DoD applications is a challenging part of the IPv6 transition. The process must be executable, affordable, and must not substantially impact ongoing DoD operations.

For applications, decisions must be made as to whether the applications can be ported into IPv6 via a COTS upgrade or whether the applications need custom modifications. A decision also must be made with regard to IPv6 functionality. Analysis should be performed on the applications to determine whether it would be valuable to leverage features of IPv6 into an existing application. Automated tools are available to support the

[5] For this plan, the term “Application” includes most software such as databases and computer operating systems.

porting process. Capabilities and applicability of these tools must be evaluated in the context of the requirements.

The DITO shall provide guidelines regarding the modification of application logic, Application Program Interface (API) calls, and software configuration item and application-level test and verification. In addition, the DITO should provide technical assistance to DoD Components in application transition efforts. The DITO has developed an Application Engineer Guidebook to assist DoD Components in planning and evaluating application transition efforts.

Applications that require modification to achieve IPv6 capability should work in both IPv4 and IPv6 environments. In transitioning these applications, developers must account for modified API calls required in an IPv6 environment and new IPv6 API calls for the new features of IPv6. Application software being developed should also be implemented in a way that isolates the network (IP) layer as much as possible from the rest of the application. This will help facilitate incorporating changes as IPv6 features continue to mature.

A.7 Standards

Standards relating to IPv6 are developed by the IETF. Although most of the core set of IPv6 standards are stable and mature, work is still underway in the IETF in key areas[6] such as mobile IPv6, multi-casting, anycast, flow label, multi-homing, security, network management, and transition mechanisms. As the DoD's Executive Agent for IT standards, DISA is engaged with the standards bodies, such as the IETF in the evolution and finalization of the IPv6 standards and features needed by the DoD. The DITO is responsible for ensuring that standards needs and concerns are identified and addressed through participation with industry in the IETF and/or other appropriate forums.

The DoD IT Standards Registry (DISR) is a reference document that mandates a set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The DISR is to be used by anyone involved in the management, development, or acquisition of new or improved systems within the DoD. Since the DISR is a living document, the DoD shall ensure that newly-released IPv6 standards (with implementations) are incorporated in DISR revisions in a timely manner using the established DISR process. The Standard Profiles for IPv6 Capable Products has been placed on the DISR and is available online (http://disronline.disa.mil).

A.8 Advanced IPv6 Capabilities

While the base IPv6 protocol is considered mature and standardized, standardization and implementation work is on-going in the IETF in QoS, mobility, and network management

[6] It is important to remember that IPv6 will continue to evolve even when it is widely implemented. Even today, IPv4 standards work is still ongoing within the IETF.

and other value-added applications. It is important that DoD requirements and needs are well understood for the evolving IPv6 standards. The DITO is currently funding the following efforts for key DoD GIG applications that will benefit from IPv6 technology.

- Quality of Service (QoS) and Multi-Level Precedence and Preemption (MLPP) in IPv6 Networks – in the GIG, all traffic must be provided with precedence level options. This requirement is also called Multi-Level Priority and Preemption. Realization of MLPP is more efficient in IPv6 because of availability of a Flow Label Field. Currently, there is no consensus on how to best utilize these tools to implement MLPP.

- IPv6 network mobility with minimum re-configurations – to achieve ubiquitous IP connectivity, the DoD will need efficient mobility support mechanisms to maintain ongoing communication flows while on the move. Such mechanisms include host mobility support (displacement of a single host in the IP topology without breaking open sessions), network mobility support (displacement of an entire network in the IP topology without breaking open sessions), and ad hoc networking (routing in an infrastructure-less network). These mechanisms are needed in addition to core IPv6 technologies such as multi-homing, auto-configuration, multicast, security, and access control. The combination of all these technologies will enable mobile vehicles to connect to the IP network and soldiers and commanders carrying IP devices to keep uninterrupted access to the IP infrastructure whether they are located within tactical networks, command centers, offices, or going between networks that may be on the move themselves.

- Application of policy based network management technology to IPv6 networks – the use of Policy Based Network Management (PBNM) technology is mandated by GIG programs. This technology is deemed essential for net-centric operations. PBNM can automate the operations, thus enhancing efficiency and consistency, reducing errors, and saving cost. More importantly, it is the practicable technology that allows dynamic near-real-time response to changing operations. In this capacity, applications based on PBNM technology will observe theater operations and adjust the supporting infrastructure automatically to the changing resource availability profiles and user needs. This helps to alleviate bandwidth constraints on theater operations.

- IPv6 in low-bandwidth systems – the DoD's tactical and highly-mobile environments provide the most network challenges for the IPv6 transition. The wireless network bandwidth will continue to be constrained until the new transformational satellite communications capabilities are operational. Therefore, the network overheads must be minimized across the tactical environments. This requires efficient header compression techniques and solutions for IPv6 implementation.

A.9 Training

Training is an essential aspect of IPv6 transition given that IPv6 is a new technology without a strong knowledge base in the DoD technical community. To achieve successful IPv6 transition, special efforts must be made to educate and train the affected DoD Components, technical and management staff. The goal of training is to give end-users the specific knowledge they need to be effective and an understanding of the end-to-end enterprise view of IPv6, which will support the DoD in transitioning from IPv4 to IPv6. Those end-users include system developers and integrators, network operations and management staff and information security managers. To implement IPv6 effectively, DoD Components will need to prepare staff for what could be substantial change. This preparation will result in a diverse and complex set of training needs. For example, systems managers must learn how to configure and manage IPv6 on network devices and upgrade servers to IPv6. Program managers and acquisition executives will need information in order to evaluate and purchase IPv6 capable products. Software developers will need details on how to make code IPv6 compatible and software updates or patches that need to be applied to make software run on IPv6. Network managers and operators will need to know how to make IPv6 work, including in a mixed IPv4/IPv6 environment. Those responsible for IA will need information on IPv6 security vulnerabilities. Another IPv6 training challenge is to coordinate IPv6 efforts within the DoD Components to incorporate these new elements into current DoD Component and joint training programs without creating redundancies.

The DITO can assist in providing coordination, guidance, and knowledge transfer of IPv6 information. The DITO has developed IPv6 program manager, network engineer and application engineer guidebooks and tool kits. In addition, the DITO has developed milestone objective implementation guidelines, including IA and network deployment guidelines. The DITO also developed workshop material for application engineers' training. This material is available for the DoD Component use. The DITO will post the available training material via a DoD IPv6 web site. DoD Components will develop training materials to satisfy their unique needs.

Appendix B: References

1. DoD CIO Memorandum, Internet Protocol Version 6 (IPv6), June 9, 2003

2. DoD CIO Memorandum, Internet Protocol Version 6 (IPv6) Interim Transition Guidance, September 29, 2003

3. DoD CIO Memorandum, Internet Protocol Version 6 (IPv6) Policy Update, August 16, 2005

4. Office of Management and Budget (OMB) Memo, Transition Planning for Internet Protocol Version 6 (IPv6), August 2, 2005

5. Department of Defense Directive 5000.1, The Defense Acquisition System, May 12, 2003

6. Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System, May 12, 2003

7. The Department of Defense Internet Protocol Version 6 Master Test Plan, Version 1.0, September 23, 2005

8. DISA (JITC) Internet Protocol version 6 Generic Test Plan (GTP), September 2005

9. DoD Internet Protocol Version 6 (IPv6) Network Engineer Guidebook, v1.1 draft, DITO, September 2005

10. DoD Internet Protocol Version 6 (IPv6) Applications Engineer Guidebook, v1.1 draft, DITO, July 2005

11. DoD Internet Protocol Version 6 (IPv6) Program Manager Guidebook, v1.2 draft, DITO, March 2006

12. DoD Internet Protocol Version 6 (IPv6) Milestone Objective 1 (MO1) Implementation Guidance, DITO, June 2005

13. DoD Internet Protocol Version 6 (IPv6) Guidance for the Information Assurance (IA) Certification and Accreditation (C&A) Process v1.1 draft, DITO, October 2005

14. Information Assurance (IA) Risk Management Process v1.1 draft, DITO, May 2005

15. Guidance for Internet Protocol Version 6 (IPv6) Information Assurance (IA) Policy, v1.1 draft, DITO, November 2005

16. Internet Protocol Version 6 (IPv6) Guidance for Information Assurance (IA) Requirements, v2.6.2 draft, DITO, December 2005

17. Information Assurance (IA) Guidance for Milestone Objective 1 (MO1), Version 1.0, DITO, January 2006

18. Information Assurance (IA) Guidance for Milestone Objective 2 (MO2) draft, DITO, February 2006

19. Guidance for Information Assurance (IA) Toolkit draft, DITO, April 2006

20. Guidance for Internet Protocol Version 6 (IPv6) Information Assurance (IA) Audit, v1.0 draft, DITO, May 2006

21. DISA Internet Protocol Version 6 (IPv6) Implementation Plan, Version 1.0, February 28, 2006

22. IETF RFC 2460, Internet Protocol Version 6 (IPv6) Specification, December 1998

23. IETF RFC 1454, Comparison of Proposals for Next Version of IP, May 1993

24. DoD IT Standards Registry (DISR): https://disronline.disa.mil/DISR/index.jsp

25. JITC APL: http://jitc.fhu.disa.mil/adv_ip/register/register.html

Appendix C: Acronyms

ADNS	Automated Digital Network System
API	Application Program Interface
APL	Approved Products List
ARIN	American Registry for Internet Numbers
ASD	Assistant Secretary of Defense
ATO	Authority to Operate
AUTH	Authentication
C&A	Certification and Accreditation
CAE	Component Acquisition Executives
CDD	Capabilities Development Document
CEA	Consumer Electronics Association
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
COMM	Communications
CONUS	Continental United States
COTS	Commercial Off the Shelf
CPD	Capabilities Production Document
DIA	Defense Intelligence Agency
DICAST	DoD Intelligence Community Accreditation Support Team
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DoD IT Standards Registry
DITO	DoD IPv6 Transition Office
DNS	Domain Name Service
DoD	Department of Defense
DOT&E	Director, Operational Test & Evaluation
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel and Facilities
DREN	Defense Research and Engineering Network
DSN	Defense Switched Network
EUR	Europe
FCS	Future Combat Systems
FY	Fiscal Year
GBS	Global Broadcast System

GIG	Global Information Grid
GOTS	Government Off The Shelf
GTP	Generic Test Plan
HAIPE	High Assurance IP Encryptors
IA	Information Assurance
IC	Intelligence Community
ICD	Initial Capabilities Document
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
IT	Information Technology
ITSDN	Integrated Tactical/Strategic Data Network
ITSG	IPv6 Transition Steering Group
ITU	International Telecommunications Union
JCIDS	Joint Capabilities Integration and Development System
JITC	Joint Interoperability Test Command
JTRS	Joint Tactical Radio Systems
JWICS	Joint Worldwide Intelligence Communications System
KDC	Key Distribution Center
MLPP	Multi-Level Precedence and Preemption
MO	Milestone Objective
MO1	Milestone Objective 1
MO2	Milestone Objective 2
MO3	Milestone Objective 3
MPLS	Multi-Protocol Label Switching
MTP	Master Test Plan
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NCES	Net-Centric Enterprise Services
NCOW	Net-Centric Operations and Warfare
NIAP	National Information Assurance Partnership
NIC	Network Information Center
NII	Networks and Information Integration

NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NSA	National Security Agency
NSS	National Security Systems
OMB	Office of Management and Budget
PAC	Pacific
PBNM	Policy Based Network Management
PD DoD CIO	Principal Deputy DoD Chief Information Officer
PEO	Program Executive Office
PKI	Public Key Infrastructure
QoS	Quality of Service
RFC	Request for Comment
SCI	Sensitive Compartmented Information
SIPRNet	Secret Internet Protocol Router Network
SWA	Southwest Asia
T&E	Test and Evaluation
TSAT	Transformational Communications Satellite
USJFCOM	U.S. Joint Forces Command
VPN	Virtual Private Network
WAN	Wide Area Networks