Information Technology | Federal IPv6 Task Force

Managing the IPv6 Implementation Effort

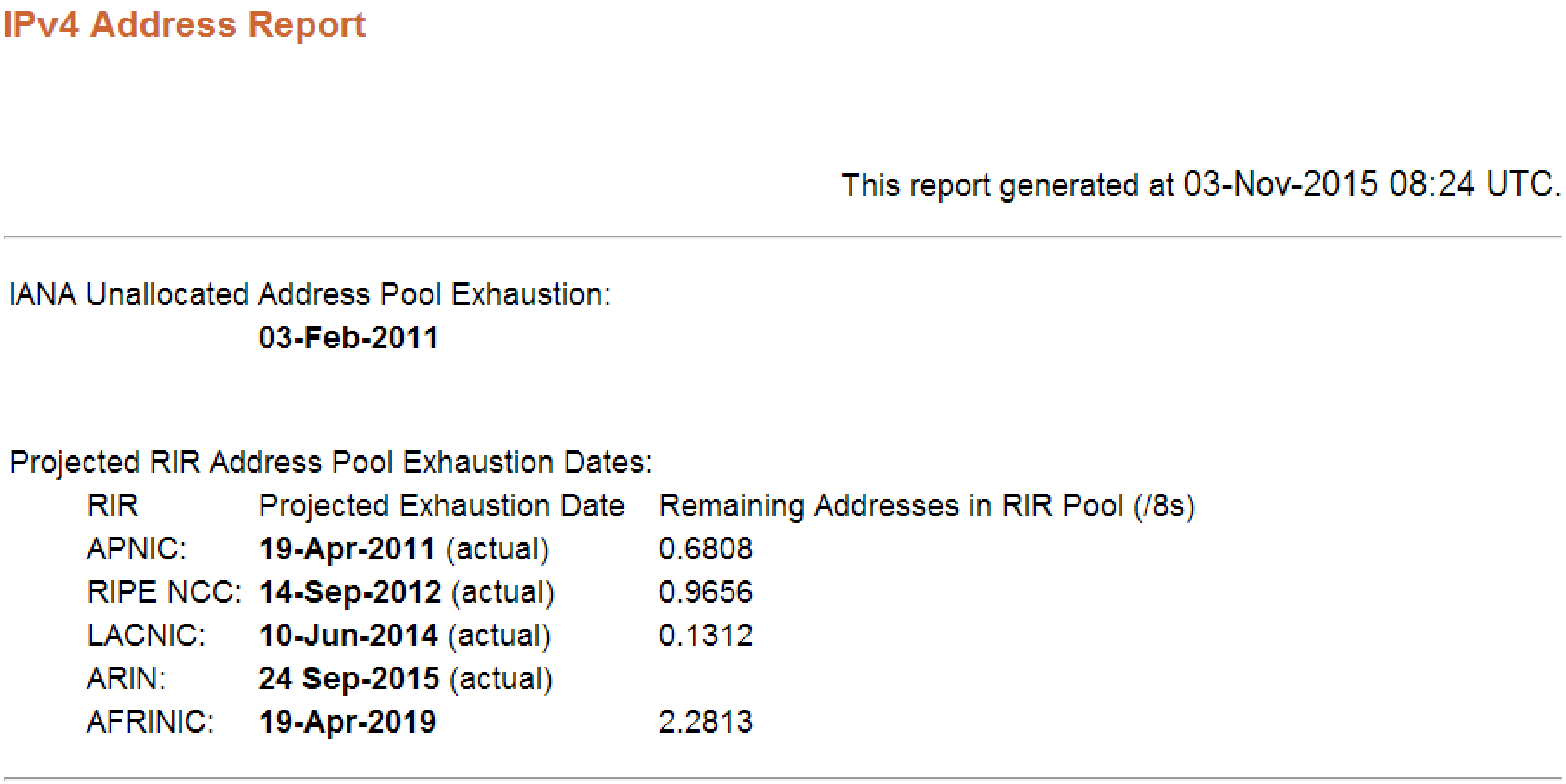
November 5th, 2015

Ralph Wallace
IRS IPv6 Transition Manager
Ralph.L.Wallace@irs.gov

Agenda

- Introduction
- Background
- Governance
- Transition Planning
- Transition Implementation
- Acquisition
- Training
- Questions

Introduction



IPv4 Address Report

This report generated at 03-Nov-2015 08:24 UTC.

IANA Unallocated Address Pool Exhaustion:

03-Feb-2011

Projected RIR Address Pool Exhaustion Dates:

RIR	Projected Exhaustion Date	Remaining Addresses in RIR Pool (/8s)
APNIC:	**19-Apr-2011** (actual)	0.6808
RIPE NCC:	**14-Sep-2012** (actual)	0.9656
LACNIC:	**10-Jun-2014** (actual)	0.1312
ARIN:	**24 Sep-2015** (actual)	
AFRINIC:	**19-Apr-2019**	2.2813

"Exhaustion" is defined here as the time when the pool of available addresses in each RIR reaches the threshold of no more general use allocations of IPv4 addresses. As ARIN have already reserved a /10 for the transition to Ipv6 policy, the low point for ARIN is a completely depleted general use pool. For AFRINIC and LACNIC the threshold is a total of a /11 remaining in their available address pool. This calculation also takes into account the redistribution of the IANA Global Address pool, and in the simulation of exhaustion these addresses are redistributed to the RIRs according to the policy.

USG Impact

- This transition touches EVERY component on the USG enterprises including
  - All websites
  - All email
  - All Switches & Routers
  - All Platform Operating Systems
  - All devices that connect to the network (e.g printers)
  - All Applications need to be tested and some may require updates
- Current USG customers using IPv4 will continue to access the USG web services and communicate via email (or until USG support for IPv4 is removed).
- Future Access of USG customers to the USG Internet Access Points must be provided for USG customers who only have IPv6 access
  - We will need to support a “dual stack” (IPv4 & IPv6 addresses) for many years as the “world” makes the transition to IPv6 (or until USG support for IPv4 is removed).
- Internal client applications such as Web Browsers on workstations must be able to access both the IPv4 and IPv6 Internets

Internet traffic accessing IRS.gov is now 15% IPv6, increasing annually by 5%

Introduction

Originating Direction -

In October 2003, the President's National Strategy to Secure Cyberspace (National Strategy) directed the Secretary of Commerce to form a task force to examine the most recent iteration of the Internet Protocol version 6 (IPv6). The President charged the task force with considering a variety of IPv6-related issues, "including the appropriate role of government, international interoperability, security in transition, and costs and benefits."

GAO-05-471 May 2005 INTERNET PROTOCOL VERSION 6
Federal Agencies Need to Plan for Transition and Manage Security Risks

OMB M-05-22 August 2, 2005
MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS
FROM: Karen S. Evans, Administrator, Office of E-Government and Information Technology
SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

IPv6 Economic Impact Assessment, October 2005
National Institute of Standards and Technology

Technical And Economic Assessment Of Internet Protocol Version 6 (IPv6), January 2006
Department of Commerce led IPv6 Task Force Findings

IPv6 Transition Guidance, February 2006
Federal CIO Council Architecture and Infrastructure Committee

Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government Version 1.0, May 2009
Issued by Federal CIO Council Architecture and Infrastructure Committee

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES, September 28, 2010
FROM: Vivek Kundra , Federal Chief Information Officer
SUBJECT: Transition to IPv6

Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government Version 2.0, July 2012
Issued by Federal CIO Council Strategy and Planning Committee

Background

GAO-05-471 May 2005 INTERNET PROTOCOL VERSION 6

"Federal Agencies Need to Plan for Transition and Manage Security Risks" (41 Pages)

GAO was asked to (1) describe the key characteristics of IPv6; (2) identify the key planning considerations for federal agencies in transitioning to IPv6; and (3) determine the progress made by the Department of Defense (DOD) and other major agencies to transition to IPv6.

GAO recommends, among other things, that the Director of the Office of Management and Budget (OMB) instruct agencies to begin to address key planning considerations for the IPv6 transition, and that agencies act to mitigate near-term IPv6 security risks.

Background

We recommend that the Director of OMB take the following two actions:

1. Instruct federal agencies to begin addressing key IPv6 planning considerations, including
    - developing inventories and assessing risks,
    - creating business cases for the IPv6 transition,
    - establishing policies and enforcement
    - determining costs, and
    - identifying timelines and methods for transition, as appropriate.

2. Amend the Federal Acquisition Regulation with specific language that requires that all information technology systems and applications purchased by the federal government be able to operate in an IPv6 environment.

Because of the immediate risk that poorly configured and unmanaged IPv6 capabilities present to federal agency networks, we are recommending that agency heads take immediate actions to address the near-term security risks, including determining what IPv6 capabilities they may have, and initiate steps to ensure that they can control and monitor IPv6 traffic.

Background

OMB 05-22, August 2, 2005

Attachment C: Transition Activities (Notional Summary of CIO Council Guidance)
The CIO Council will develop additional transition guidance as necessary covering the following actions. To the extent agencies can address these actions now, they should do so.
Beginning February 2006, agencies' transition activity will be evaluated using OMB's Enterprise Architecture Assessment Framework:

- Conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements.
- Develop a sequencing plan for IPv6 implementation, integrated with your agency Enterprise Architecture.
- Develop IPv6-related policies and enforcement mechanisms.
- Develop training material for stakeholders.
- Develop and implement a test plan for IPv6 compatibility/interoperability.
- Deploy IPv6 using a phased approach.
- Maintain and monitor networks.
- Update IPv6 requirements and target architecture on an ongoing basis.

Background

IPv6 Transition Guidance, February 2006 (37 pages) Federal CIO Council

4.2 Components of an IPv6 Transition Plan

The following is a list of components that could be used as the basis for an IPv6 transition plan. Although agencies are not required to include all of these components in their transition plan, it is recommended that agencies cross-check their own plan against this list to ensure no critical transition elements have been overlooked.

1. Identification of strategic business objectives
2. Identification of transition priorities
3. Identification of transition activities
4. Transition milestones
5. Transition criteria for legacy, upgraded, and new capabilities
6. Means for adjudicating claims that an asset should not transition in prescribed timeframes
7. Technical strategy and selection of transition mechanisms to support IPv4/IPv6 interoperability
8. Management and assignment of resources for transition
9. Maintenance of interoperability and security during transition
10. Use of IPv6 standards and products
11. Support for IPv4 infrastructure during and after 2008 IPv6 network backbone deployment
12. Application migration (if required to support backbone transition)
13. Costs not covered by technology refresh
14. Transition governance
    a. Policy
    b. Roles and responsibilities
    c. Management structure
    d. Performance measurement
    e. Reporting
15. Acquisition and procurement
16. Training
17. Testing

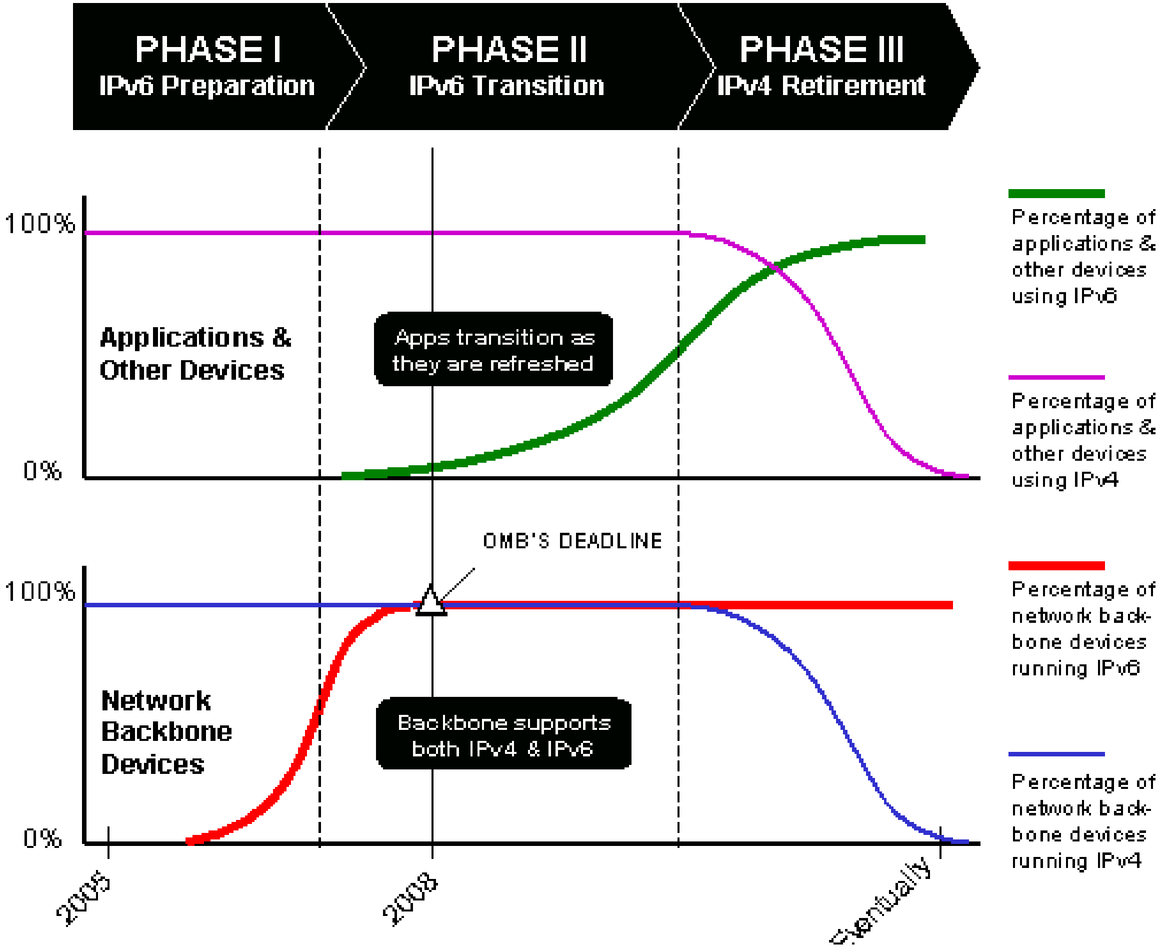
Background

From “Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government “, Version 1.0, May 2009

A. Transition will happen in 3 phases

B. Most Application software and non-backbone devices will automatically switch to IPv6 when they are upgraded / refreshed

C. Network backbone devices will support both IPv4 & IPv6 network communications while applications & other devices transition



Background

Department of Education's take on the Transition Guidance (Released 2011)

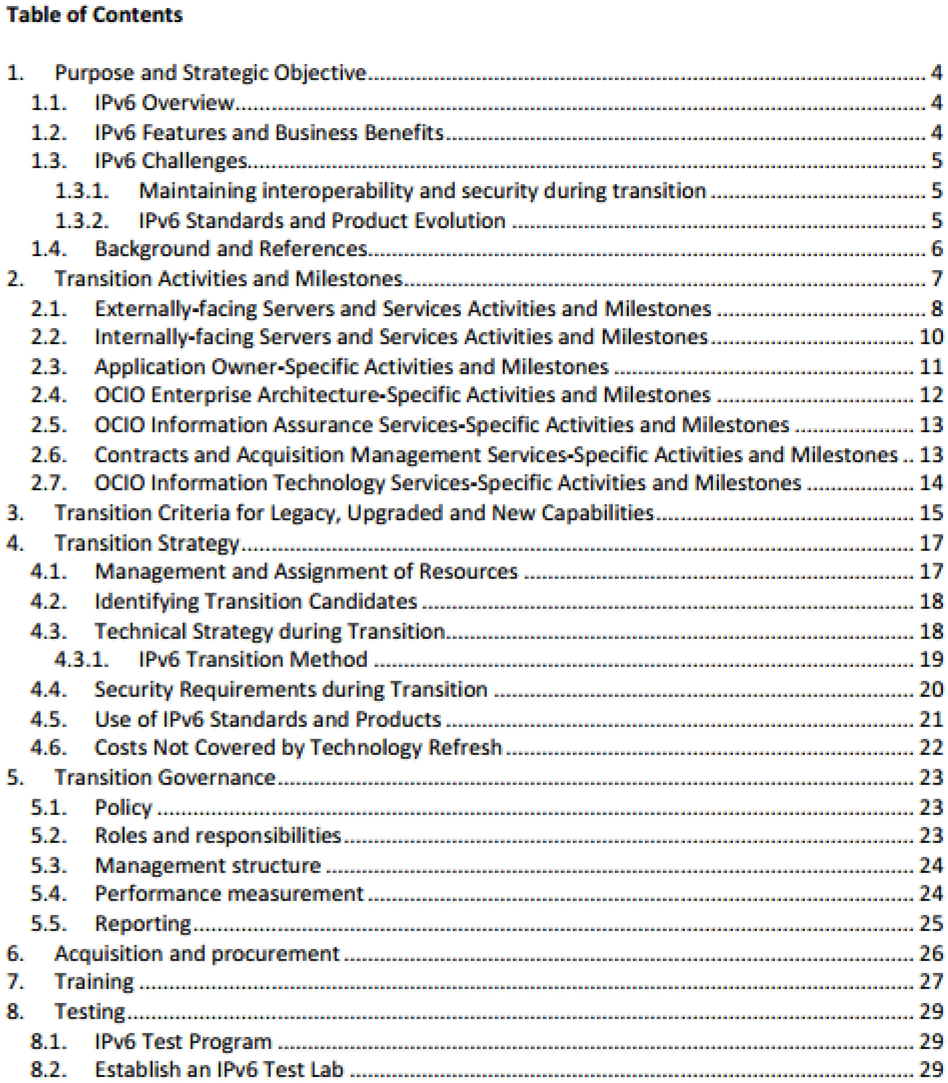


Table of Contents

Background

IRS take on the Transition Guidance (Released 2012, updated 2015)

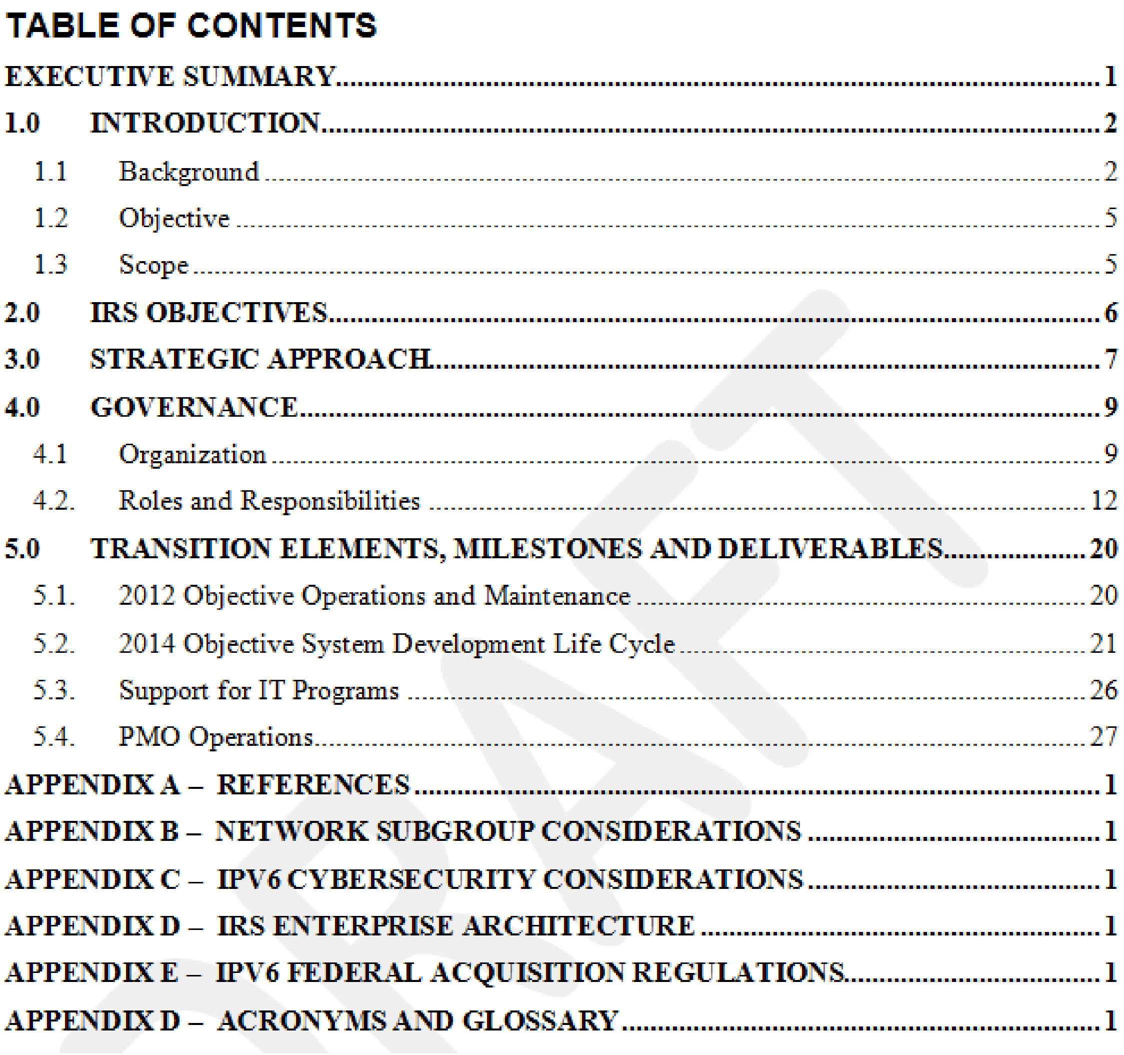


TABLE OF CONTENTS

Transition Planning

Establish Objectives

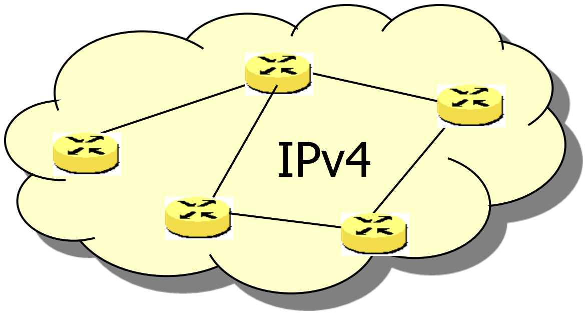
Primary focus for 2012 Objective: Websites, Email and External DNS
Primary focus for 2014 Internal client applications that require the Internet to accomplish their business function (e.g. FTP servers, Internet browsers)
Strategic Initiative: Remove reliance on IPv4 enterprise-wide as soon as it is reasonable and prudent

Establish Approach

Agency-wide Transition Manager with assigned authority to conduct efforts between IT and Business Unit organizations.
Central Transition Management PMO with corresponding IPT
Establish functional areas to establish and sustain focus
Establish functional objectives in each area supporting the overarching objectives

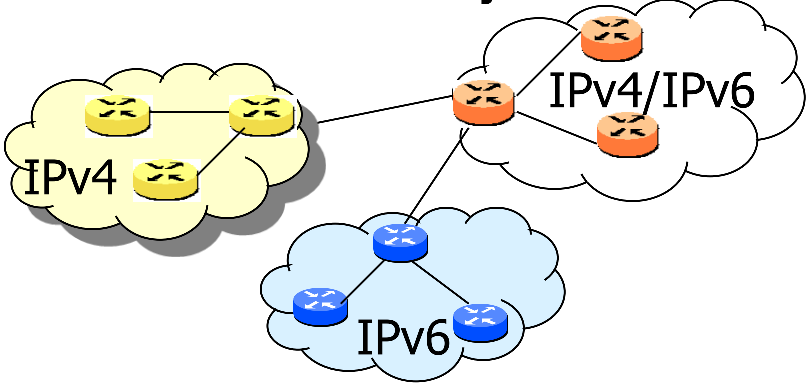
Objectives

Pre-2012



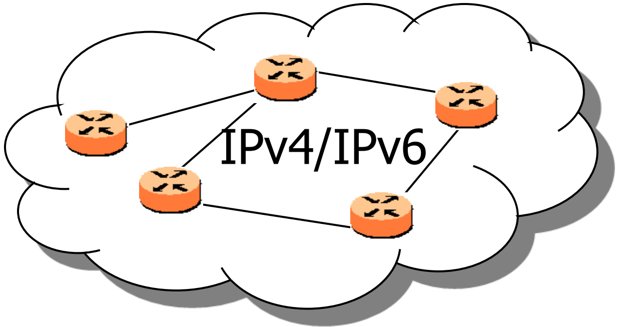
IPv4-only Network

2014+ Objective



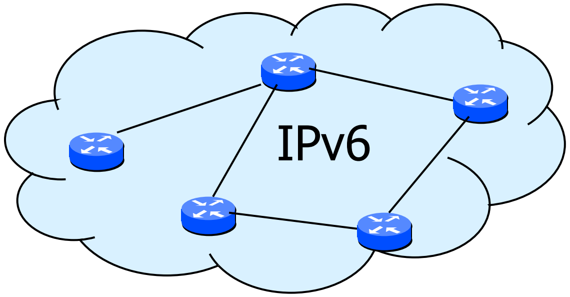
Heterogeneous Network

Post-2012 Internet Facing



Dual Network

Strategic Initiative



IPv6-only Network

Governance

Oversight
Business Processes
Risk Management
Collaboration across organizations
Assigned responsibility, authority and accountability
Appropriate delegation
Phased approach
Agreed on expected outcomes

Your agency’s structure? CMMI, ITIL, ISO, Agency-specific?

Governance

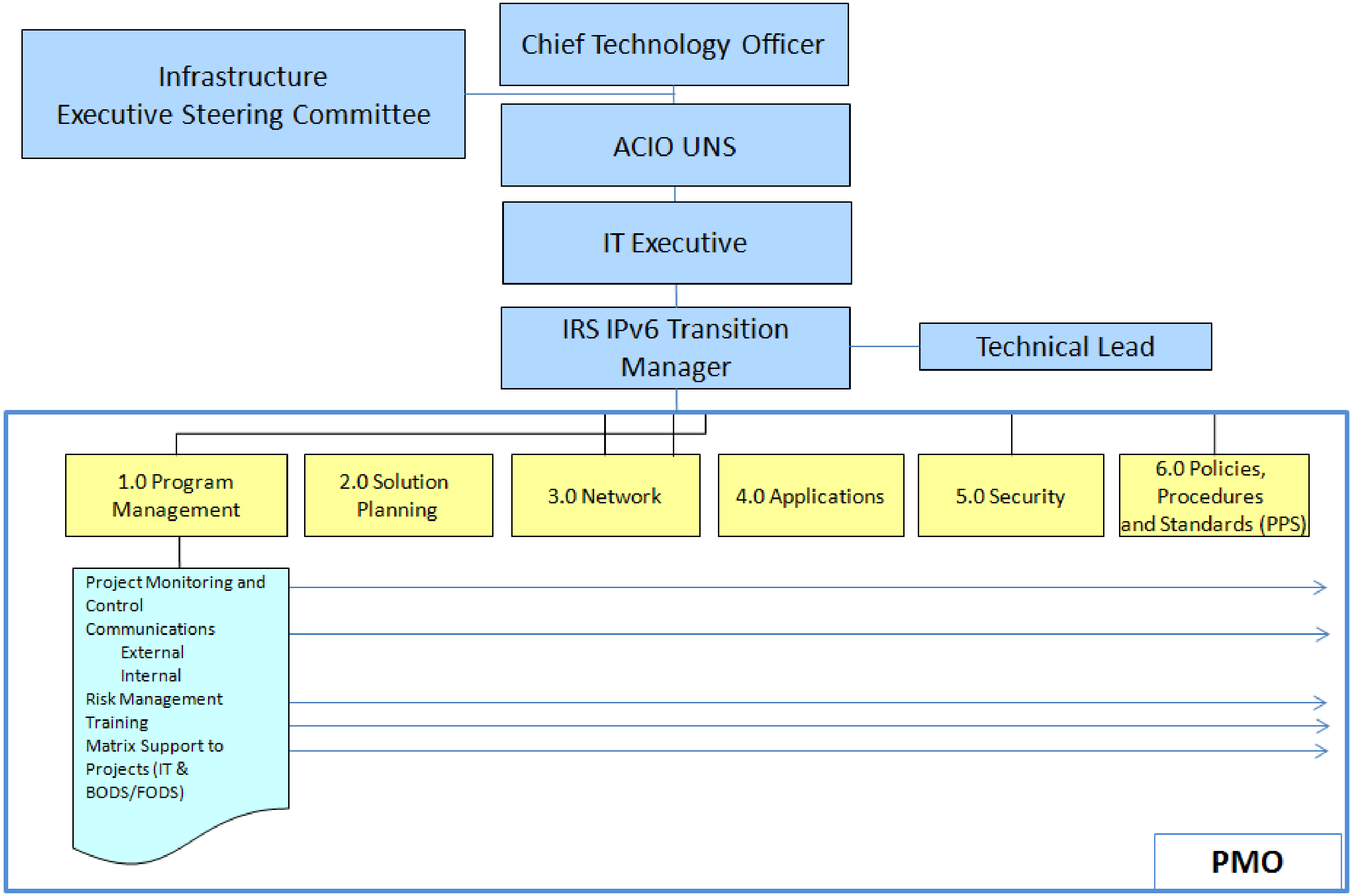


Figure : Strategic Approach for IPv6 within IRS Enterprise

Revised May 2015

Governance

- Network Subgroup
  - IPv6 Address Management
  - Routers
  - Switches
  - DHCPv6
  - DNS
  - Load Balancer
  - Platforms (Client and Server)
    - MS
    - Linux
    - Unix
  - Locater ID Separation Protocol (LISP)
  - WAN, MAN, LAN, PAN architecture

Governance

Cyber-Security Subgroup

Concerns

- Running two protocols simultaneously makes an organization vulnerable to the sum of both protocol issues
- Need to evaluate existing security models
- Need to control tunneling
- Possible misuse of autoconfiguration and control capabilities

Governance

Cyber-Security Subgroup

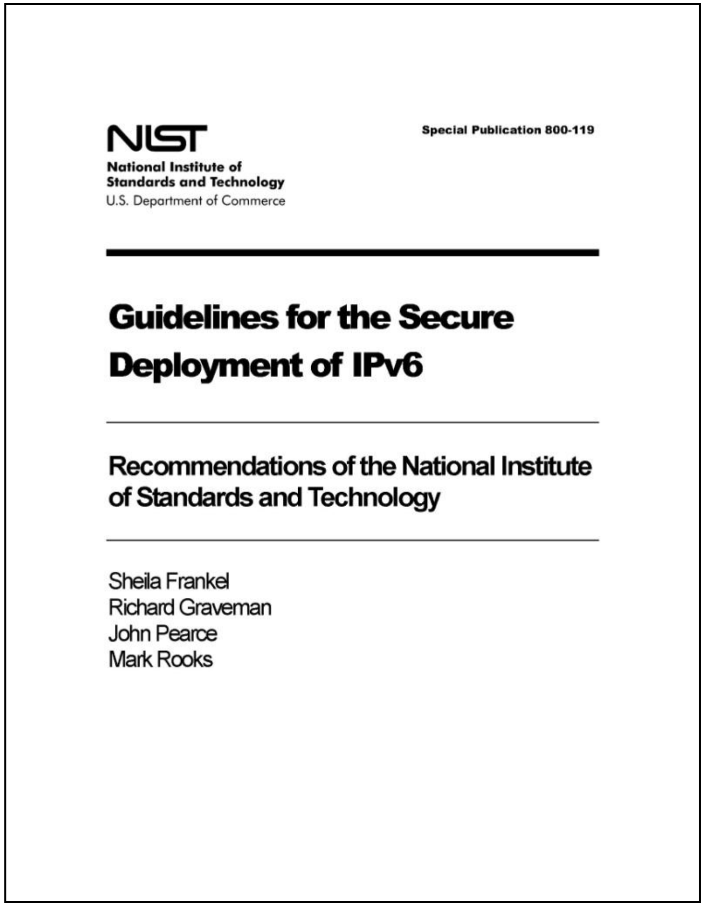
- Firewalls
- Proxies
- Deep Packet Inspection (DPI)
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Access Control Lists (ACLs)
- RA Guard
- Address Planning
- Host firewalls
- Policies and Procedures
- Architecture Design
    - Perimeter
    - Infrastructure
    - Host

Governance

Guidelines for Secure Deployment of IPv6

(NIST Special Publication 800-119)

- Addresses operational issues of IPv6 secure deployment.
- IPv6 Technology
- Security Risks
- Addressing Issues
- Transition Mechanisms
- Deployment Planning Process



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

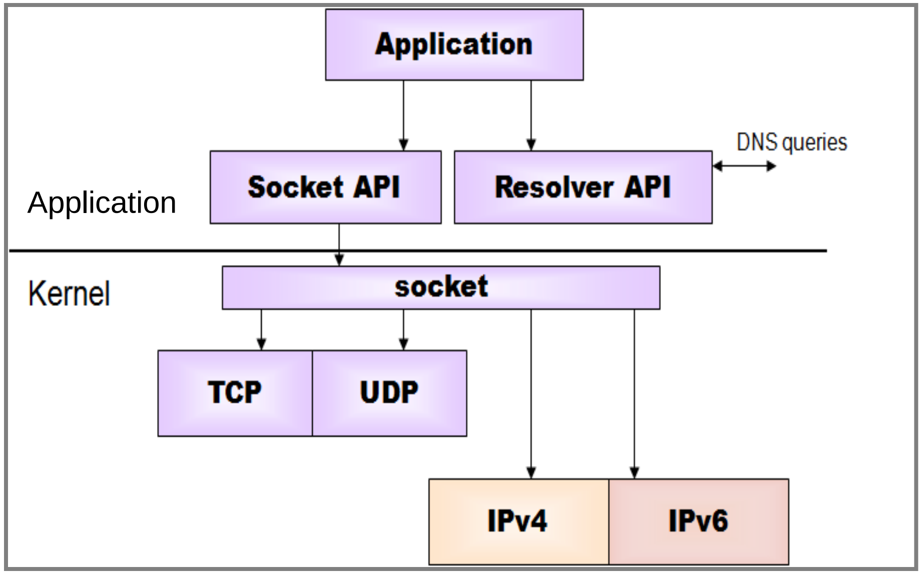
Special Publication 800-119

Guidelines for the Secure Deployment of IPv6

Recommendations of the National Institute of Standards and Technology

Sheila Frankel
Richard Graveman
John Pearce
Mark Rooks

Applications Subgroup



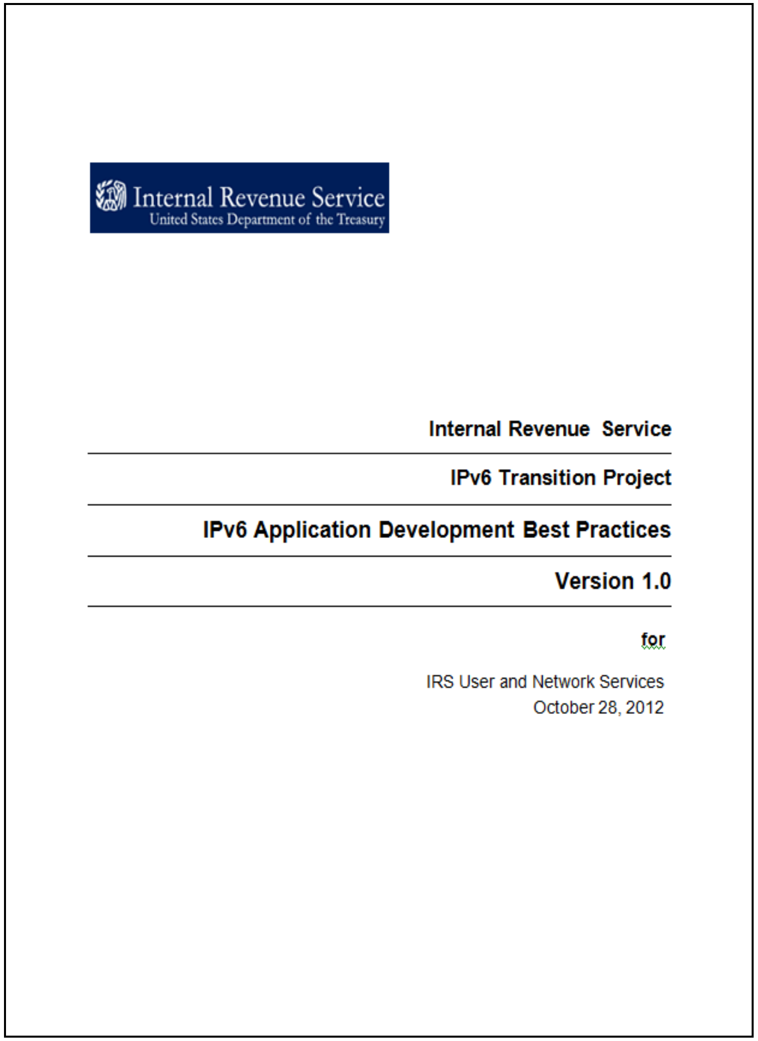
Industry experience has identified the prevalence of hard coded IPv4 addresses used to establish host to host network connections. These addresses are often neither documented in the application documentation nor the code base.

Industry best practices advise the use of DNS and DHCPv6 to effectively manage the deployment and distribution of IPv6 addresses due to the 128 bit address nomenclature, size and scope.

IRS Objective is to remove reliance on any hard coded IP addresses, and transition to use of Fully Qualified Domain Names (FQDN) to resolve hosts.

IRS End Goal is to facilitate the transition of any application from an IPv4 connection to an IPv6 environment employing DNS. This will result in reduced manual effort, decreased risk, and a higher percentage of success.

Governance



Internal Revenue Service
United States Department of the Treasury

Internal Revenue Service

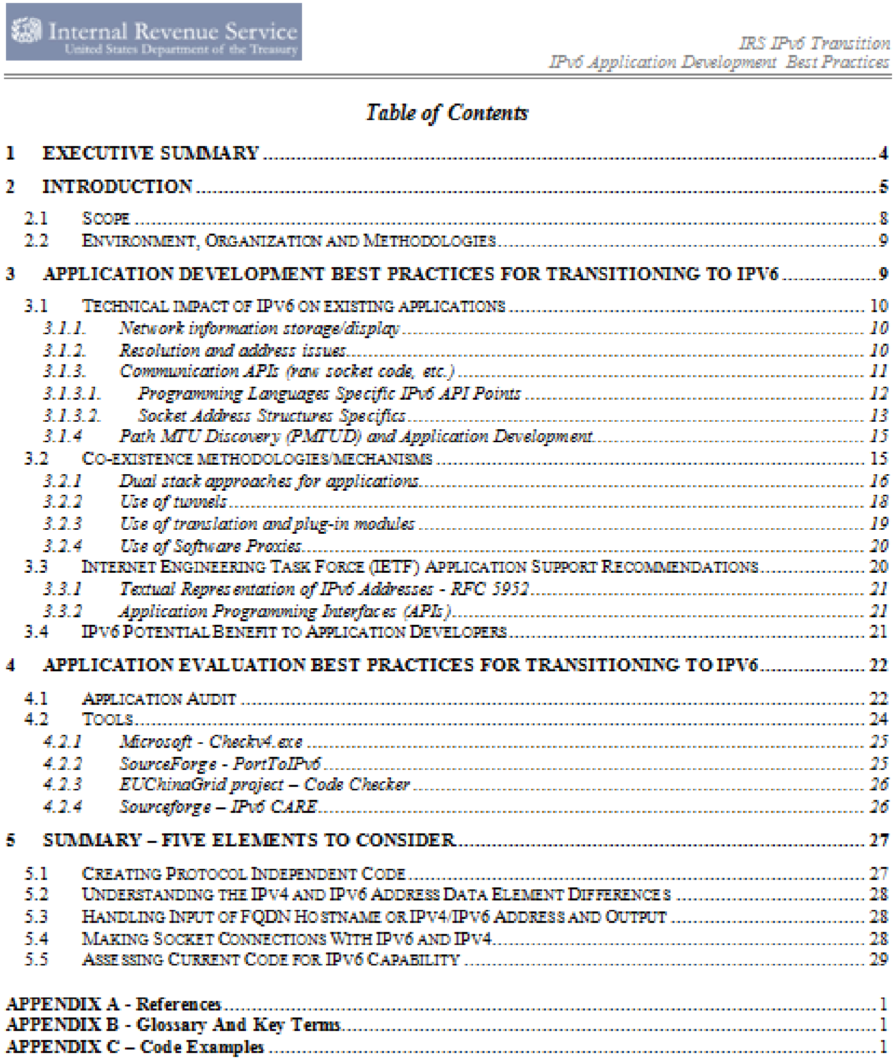
IPv6 Transition Project

IPv6 Application Development Best Practices

Version 1.0

for

IRS User and Network Services
October 28, 2012

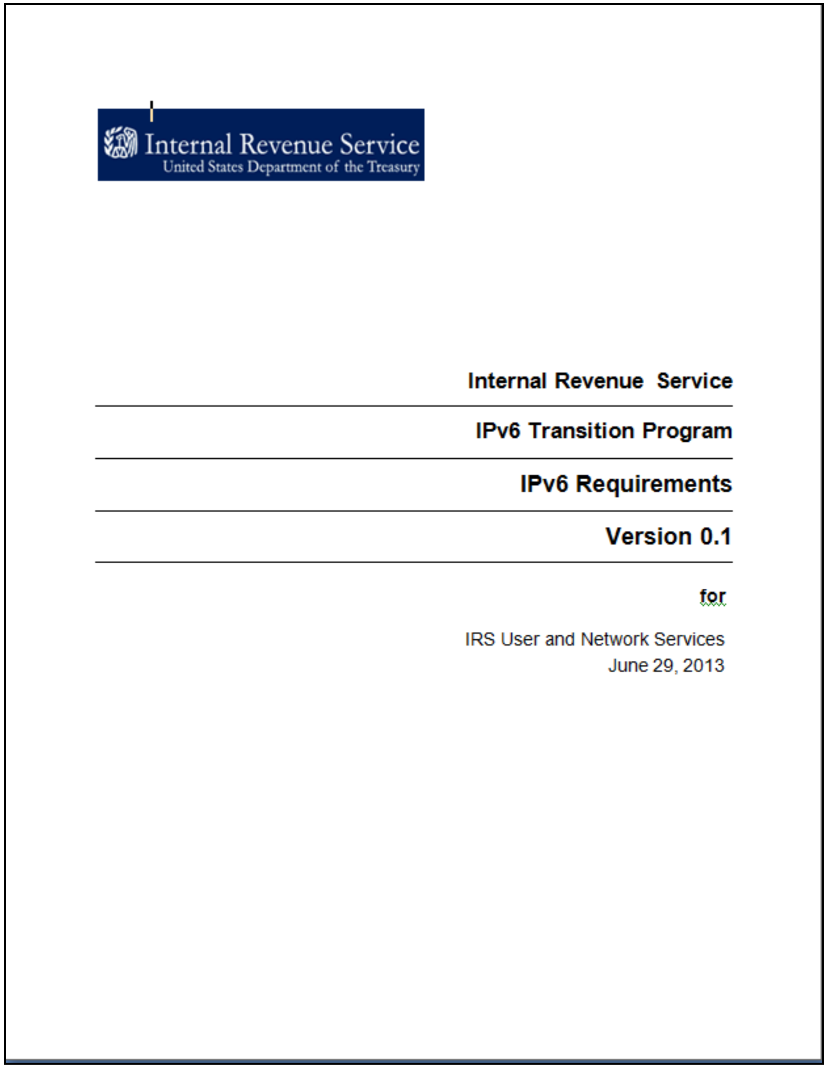


Internal Revenue Service
United States Department of the Treasury

IRS IPv6 Transition
IPv6 Application Development Best Practices

Table of Contents

Governance



Internal Revenue Service
United States Department of the Treasury

Internal Revenue Service

IPv6 Transition Program

IPv6 Requirements

Version 0.1

for

IRS User and Network Services
June 29, 2013

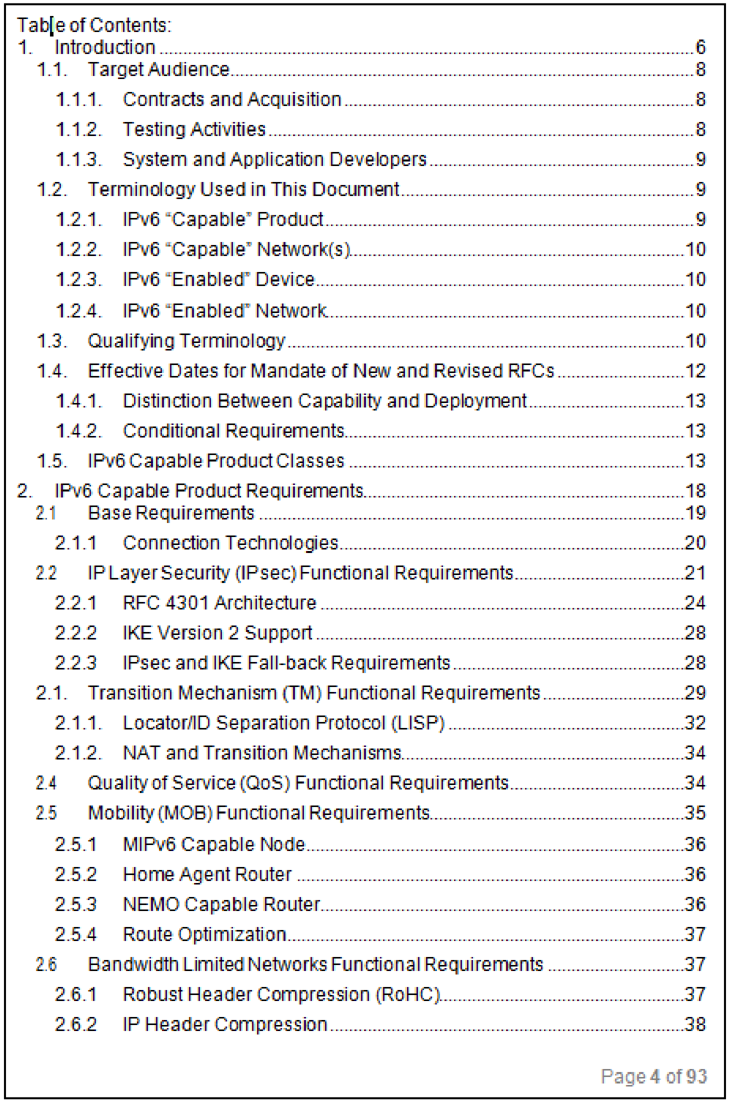


Table of Contents:

Page 4 of 93

Transition Planning

Define requirements

Determine the current state

- Assess Enterprise state of readiness (Data Calls) in the following areas in support of the 2012, 2014 and Strategic Initiative:
  - Network Infrastructure (including DHCP, DNS and platforms)
  - Cybersecurity (perimeter, infrastructure, and host)
  - Applications (external facing and internal)
  - Policy, Procedures and Standards (including FISMA Compliance)

Conduct Gap Analysis

Establish requirements, design, test, pilot and deployment workflow for each objective (Technical Lead, Solution Planning and Test Manager)

Establish respective WBS per fiscal year

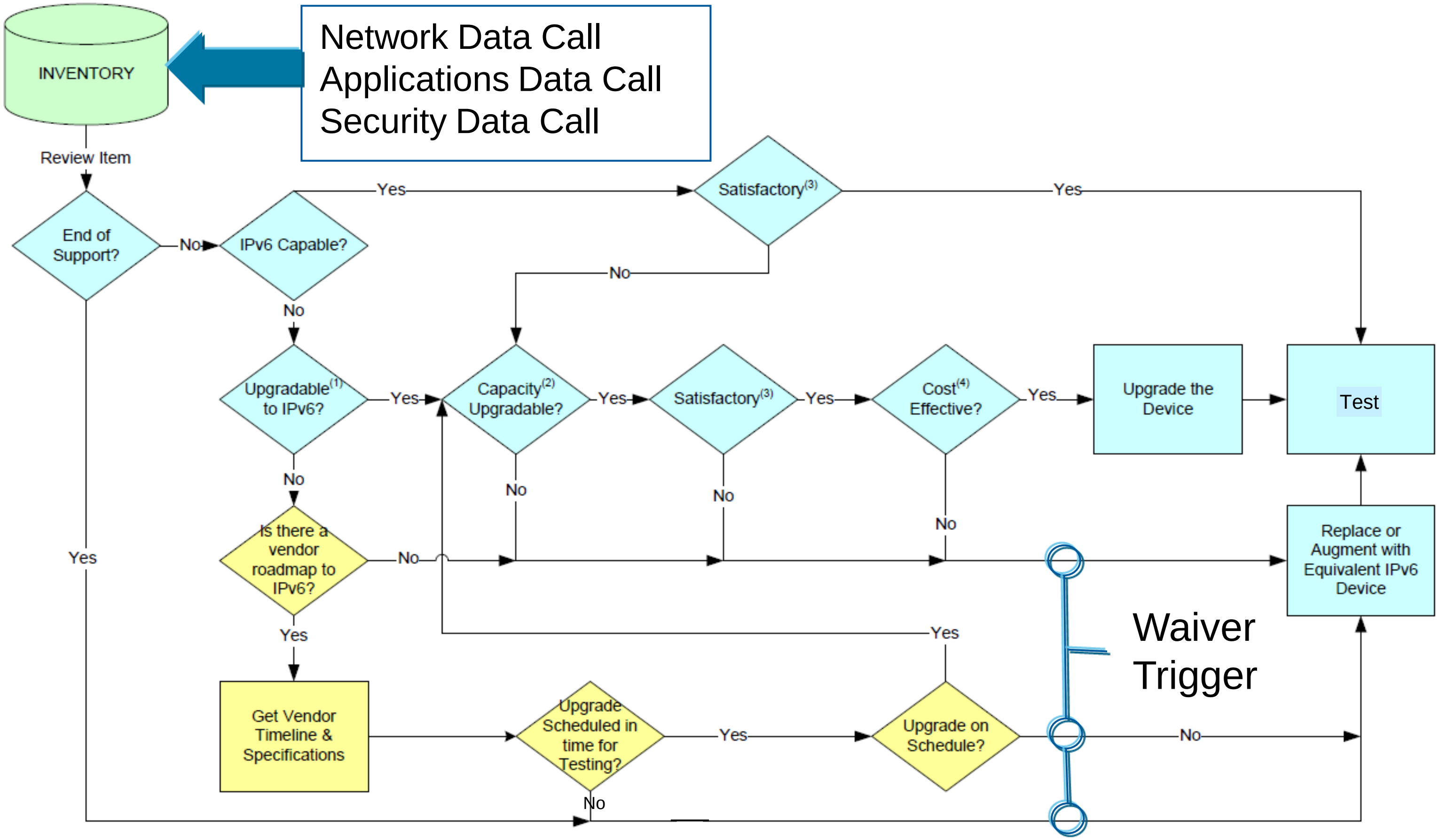
- **Schedule, Resources, Risks**

Determine Costs per fiscal year

- **Hardware, Software, Labor (including training), Risk Mitigation**

Establish budget per fiscal year

Gap Analysis



Network Data Call
Applications Data Call
Security Data Call

INVENTORY

Review Item

End of Support?

No

Yes

IPv6 Capable?

Yes

No

Satisfactory(3)

Yes

No

Upgradable(1) to IPv6?

Yes

No

Capacity(2) Upgradable?

Yes

No

Satisfactory(3)

Yes

No

Cost(4) Effective?

Yes

No

Upgrade the Device

Test

Is there a vendor roadmap to IPv6?

No

Yes

Replace or Augment with Equivalent IPv6 Device

Waiver Trigger

Get Vendor Timeline & Specifications

Upgrade Scheduled in time for Testing?

Yes

No

Upgrade on Schedule?

Yes

No

1. **Upgradable to IPv6** – The possibility of modifying a product so that it is IPv6 capable. An assumption is that after the product is upgraded it will continue to be IPv4 capable as well as IPv6.
2. **Capacity Upgradable** – The possibility of modifying an IPv6 product so that it is capable of performing in a specific use, e.g., by increasing memory capacity or processor speed.
3. **Satisfactory** – The capability of an IPv6 product to perform in a specific manner. and on schedule.
4. **Cost Effective** – The economic advisability of upgrading an IPv4 product so that it is IPv6 capable.

Transition Planning

- Establishing the Path to 2012 Technical Objective
  - Develop Addressing and Routing Plan
  - Address Acquisition
  - Establish Address Management and Allocation Procedures
  - Domain Name Service (DNS)
  - External DHCPv6
  - Platform Web Services
  - Web proxies
  - Load Balancers
  - Application Development (Preparation for 2014)
  - IPv6 Workstation Access (Preparation for 2014)
  - IPv6 workstation for Telework/VPN (Preparation for 2014)
  - Security
    - Engineering the defense in depth architecture (For 2012)
    - Complying with FISMA criteria (For 2012)
  - Governance documentation
    - Acquisition
  - Training
  - Testing

Transition Planning

- Establishing the Path to 2014 Technical Objective
  - Domain Name Service (DNS)
  - Internal DHCPv6
  - Platform Web Services
  - Web proxies
  - Load Balancers
  - Application Development in support of 2014
  - IPv6 Workstation Access
  - IPv6 workstation for Telework/VPN
  - Security
    - Engineering the defense in depth architecture (For 2014)
    - Complying with FISMA criteria (For 2014)
  - Governance documentation
    - Acquisition
  - Training
  - Testing

Transition Planning

- Establishing the Path to the Strategic Initiative
  - Establish IPv4 and IPv6 enclaves
  - Assign legacy IPv4 entities to the enclave
  - Maintain dual stack to the workstation until IPv4 is “sunset”
  - Assess readiness for applications to use IPv6
  - On designated subnets, turn off IPv4
  - Monitor IPv6 traffic
  - Security
    - Annually assess the defense in depth architecture
    - Comply with FISMA criteria
  - Governance documentation
    - Acquisition
  - Training
  - Testing

Transition Implementation

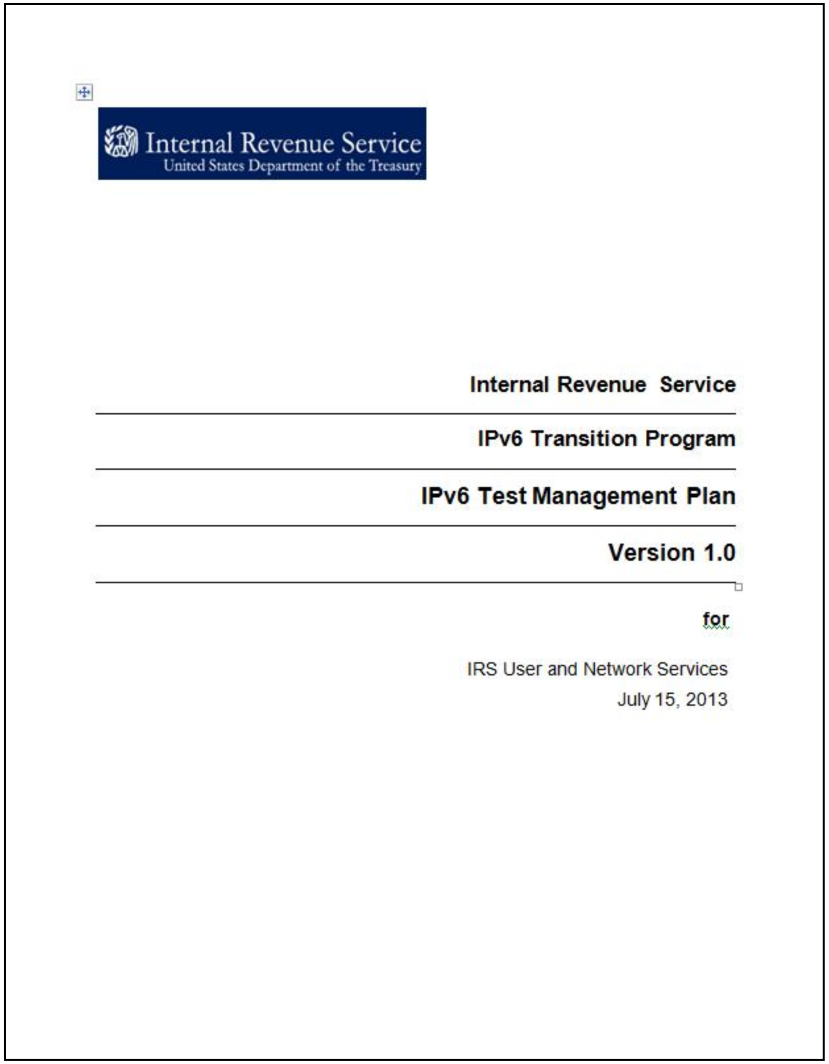
Solutions Planning Subgroup –

Deployment Process

Team	Phase / Role	Tasks
Network Subgroup	Pre-Deployment	Confirm deployment topology IPv6 “Capability”/Support IOS Upgrades
Security Subgroup	Pre-Deployment	Confirm Cybersecurity device “Capability”/ SEP12, sourcefire taps, firewall policies
Solutions Planning subgroup	Pre-Deployment	Confirm Deployment mechanisms are capable of enabling the physical topology components, and capable to establish the IPv6 routing per deployment objectives/ Coordinate phased approach
Technical Lead	Pre-Deployment	Confirm deployment methodology is validated during production proof-of-concept activities; Confirm IPv6 Addressing plan actions are properly represented within InfoBlox; Confirm LISP architecture supports IPv6 traversal of WAN./ Hands-on for phase one and two
Applications subgroup	Pre-Deployment	Identify the platforms containing IPv6 “Capable” applications, and provide to the Solutions Planning subgroup for identification and prioritization of the platforms/ support role
Solutions Planning Subgroup	Pre-Deployment	Ensure release package contains full complement of artifacts and authorizations required for deployment/ Logistics, documentation
IRS IPv6 Transition Manager	Pre-Deployment	Conduct deployment review to authorize deployment/ Monitors deployments.

Transition Implementation

IPv6 Transition Test Team



Internal Revenue Service
United States Department of the Treasury

Internal Revenue Service

IPv6 Transition Program

IPv6 Test Management Plan

Version 1.0

for

IRS User and Network Services
July 15, 2013

Transition Implementation

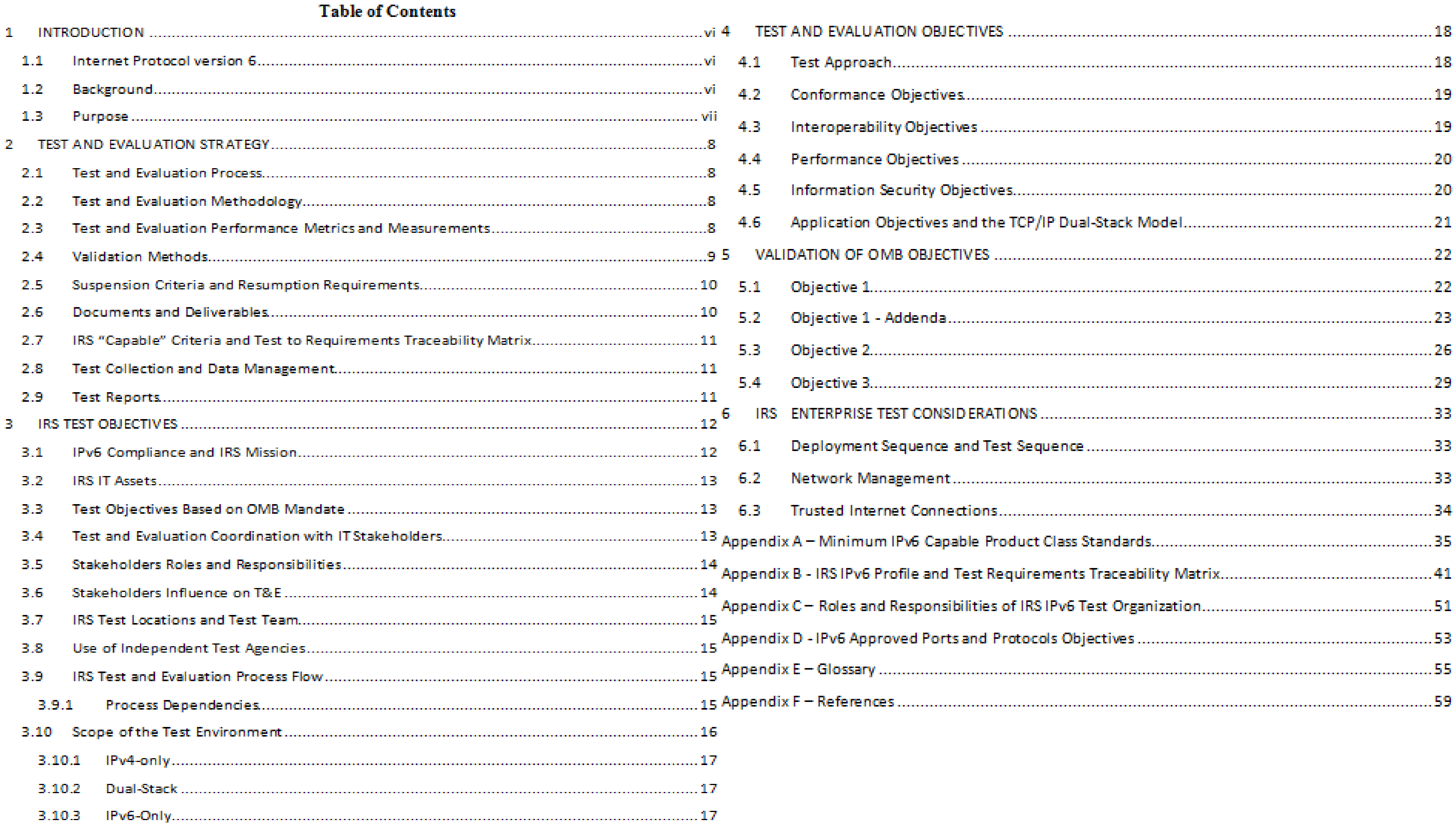
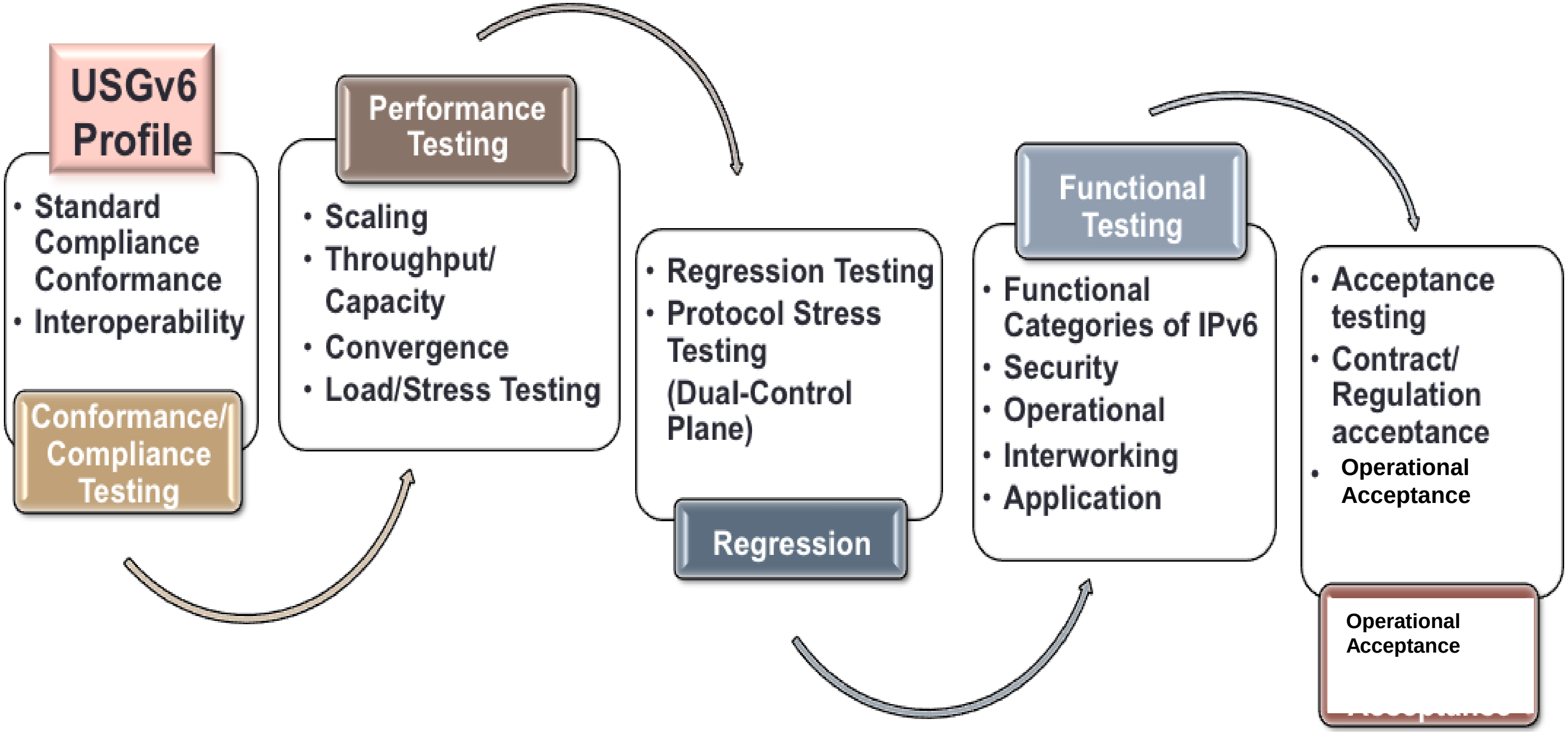


Table of Contents

IRS

Transition Implementation



USGv6 Profile

- Standard Compliance Conformance
- Interoperability

Conformance/ Compliance Testing

Performance Testing

- Scaling
- Throughput/ Capacity
- Convergence
- Load/Stress Testing

- Regression Testing
- Protocol Stress Testing (Dual-Control Plane)

Regression

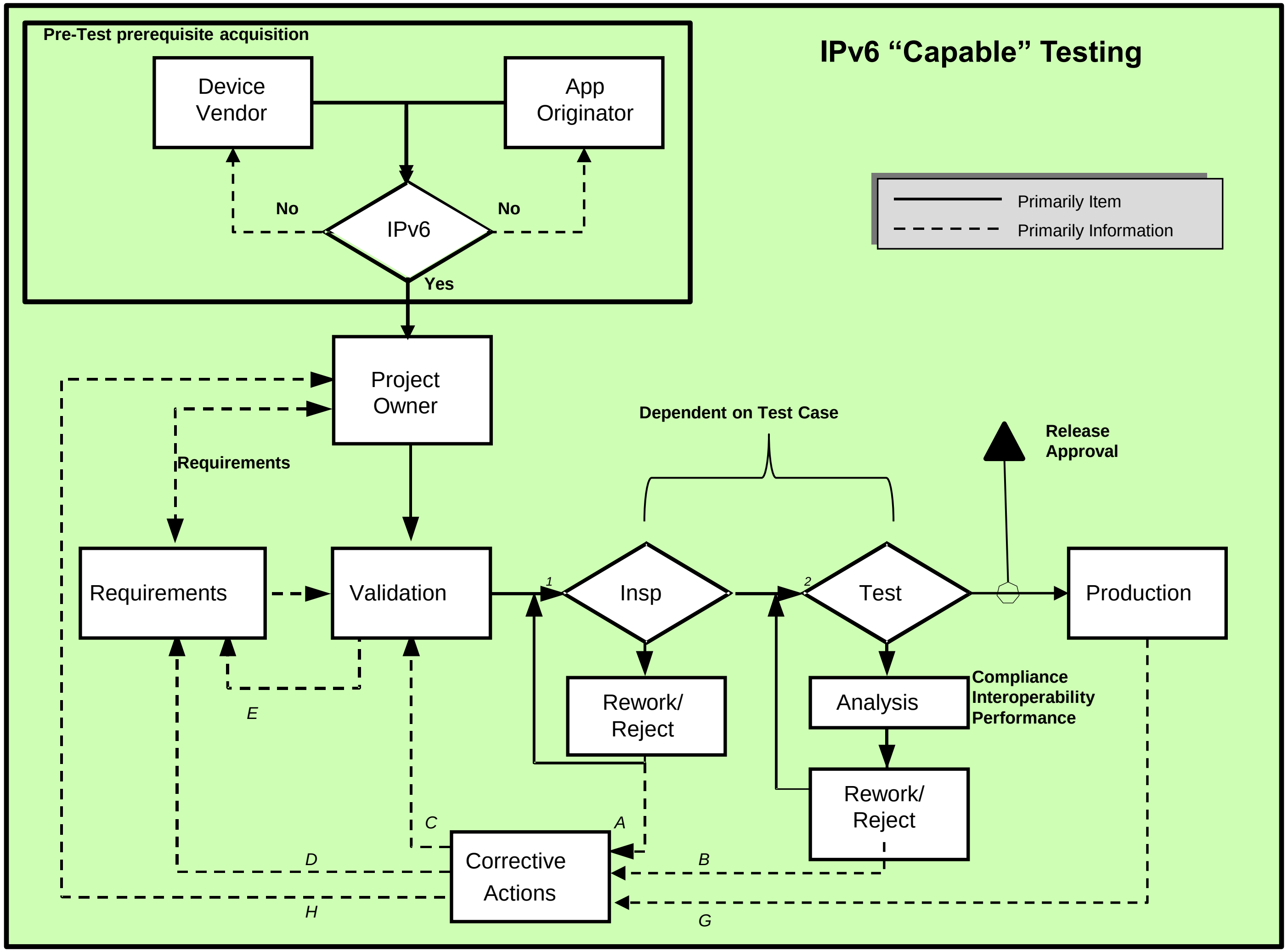
Functional Testing

- Functional Categories of IPv6
- Security
- Operational
- Interworking
- Application

- Acceptance testing
- Contract/ Regulation acceptance
- Operational Acceptance

Operational Acceptance

Transition Implementation



Acquisition

September 28, 2010

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Vivek Kundra

Federal Chief Information Officer

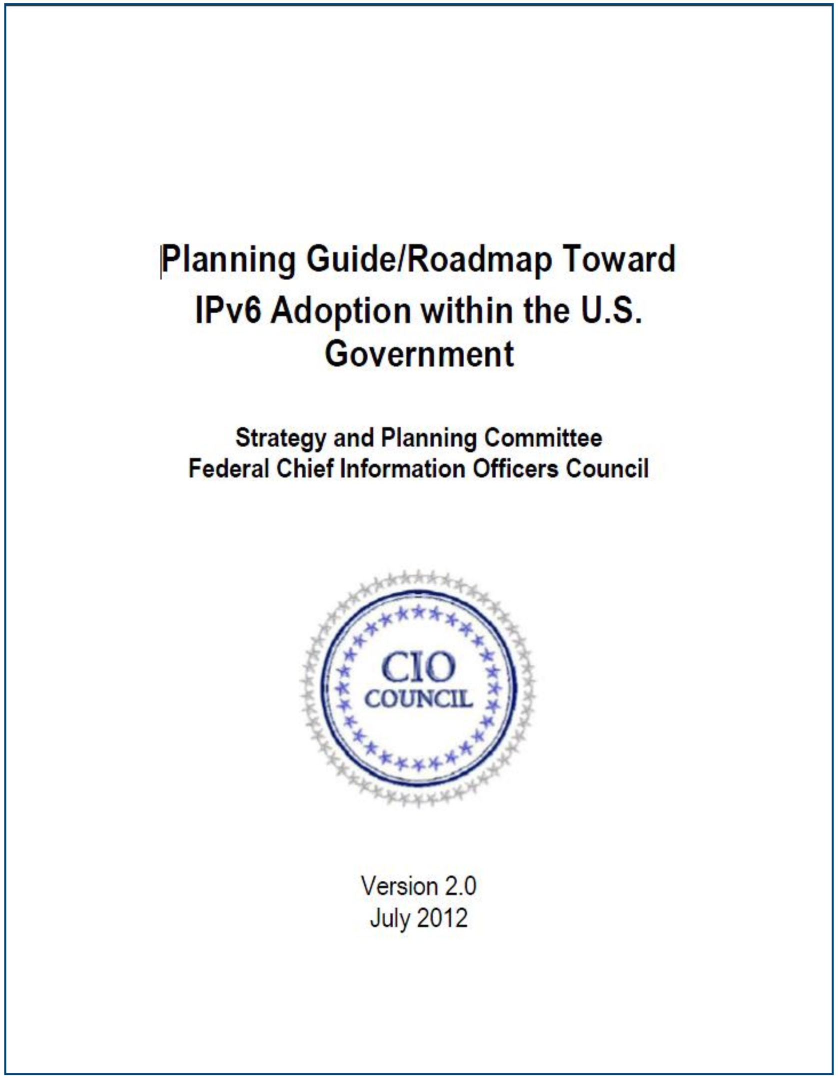
SUBJECT: Transition to IPv6

In order to facilitate timely and effective IPv6 adoption, agencies shall:

1. Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012;
2. Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;
3. Designate an IPv6 Transition Manager and submit their name, title, and contact information to IPv6@omb.eop.gov by October 30, 2010. The IPv6 Transition Manager is to serve as the person responsible for leading the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary; and,
4. ***Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.***

Acquisition

2.2 IPv6 Federal Acquisition Regulations (FAR)
DoD, GSA, and NASA published a proposed rule in the Federal Register at 71 FR 50011, August 24, 2006, to amend the FAR to ensure that all new IT acquisitions using Internet Protocol are IPv6 compliant. The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council issued a final rule amending the FAR to require that IPv6-compliant products be included in all new IT acquisitions using Internet Protocol effective December 10, 2009.



Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government

Strategy and Planning Committee
Federal Chief Information Officers Council

CIO COUNCIL

Version 2.0
July 2012

Acquisition

FAR 7.105(b)(4)
(iii) For information technology acquisitions using Internet Protocol, discuss whether the requirements documents include the Internet Protocol compliance requirements specified in 11.002(g) or a waiver of these requirements has been granted by the agency's Chief Information Officer.

FAR 11.002(g)
(g) Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. The applicability of IPv6 to agency networks, infrastructure, and applications specific to individual acquisitions will be in accordance with standards identified in the agency's Enterprise Architecture (see OMB Memorandum M-05-22 dated August 2, 2005).

FAR 12.202(e)
(e) When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with 11.002(g).

FAR 39.101(e)
(e) When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with 11.002(g).

Acquisition

2.2.2 Acquisition Guidance

It is detailed in the FAR that agency acquisition processes will be modified to include specification of required IPv6 capabilities as defined by USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program (addressed in section 2.7 of this document).

These processes and procedures also need to address procurement of services as well as products.

The acquisition of IPv4/IPv6-based network infrastructure is a collaborative effort between technical and acquisition resources, and between financial and mission management. It is recommended that cross-functional teams be impaneled to develop agency-specific processes and procedures addressing their requirements that can be updated over time, as appropriate. These services specifications are not limited to ISP services. They may also include access methods for provision of application services, including cloud provision.

Acquisition

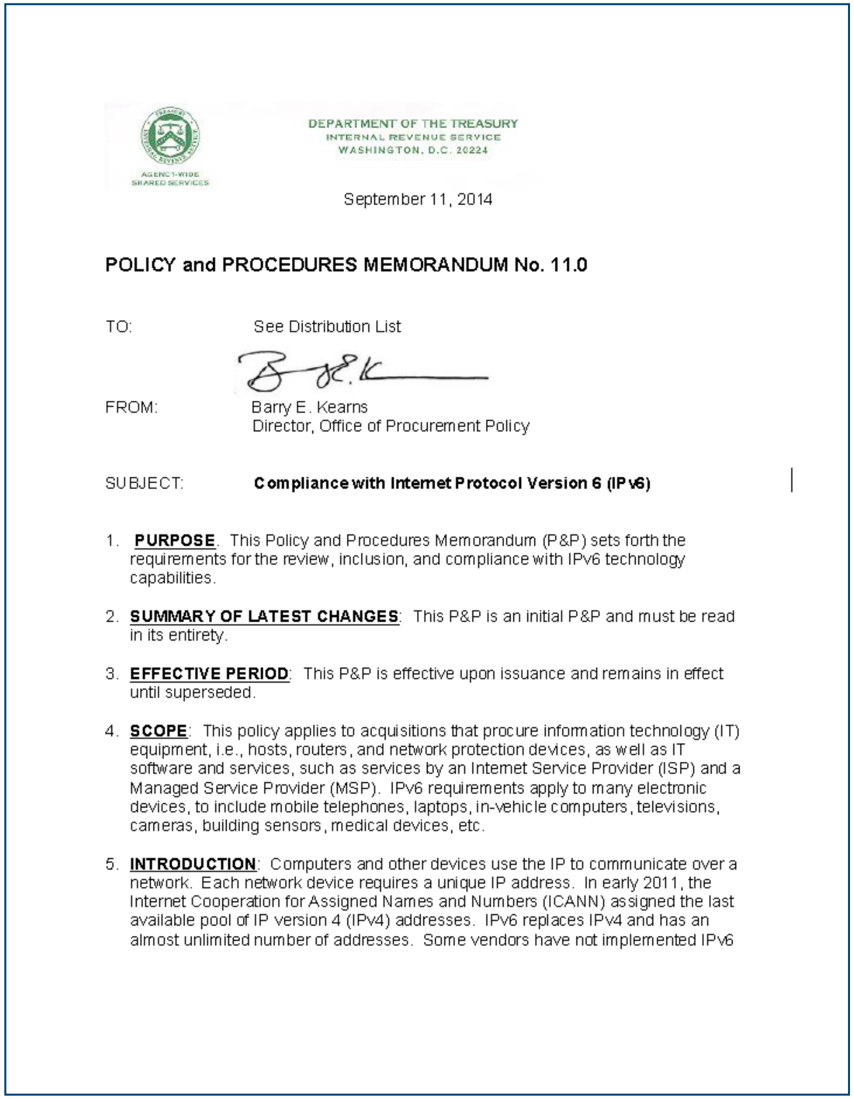
7. POLICY.
All offices and officials involved in the acquisition of IT equipment, devices, and services will follow and adhere to the policies and procedures set forth herein, regardless of the dollar value of the acquisition.

9. PROCEDURES:
A. Business Units (BUs) will:

1. Identify relevant acquisitions that require IP technical capabilities and address these capabilities within acquisition plans, statements of work or performance work statements, source selection plans, and technical evaluation plans, as deemed necessary.
2. Obtain a waiver, if the IP technical capability within the requisition documentation does not reference or include IPv6.

B. Contracting Officers (CO) will:

1. Verify that the statement of work (SOW)/performance work statement (PWS) for an IT acquisition contain an appropriate IP statement of requirements and/or specifications.
2. If the requirements are for other than IPv6 technical capabilities, the CO will direct the customer to the CTO Office identified herein for the purposes of including the requirements or assisting the customer in obtaining a waiver from them.



AGENCY-WIDE
SHARED SERVICES

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

September 11, 2014

POLICY and PROCEDURES MEMORANDUM No. 11.0

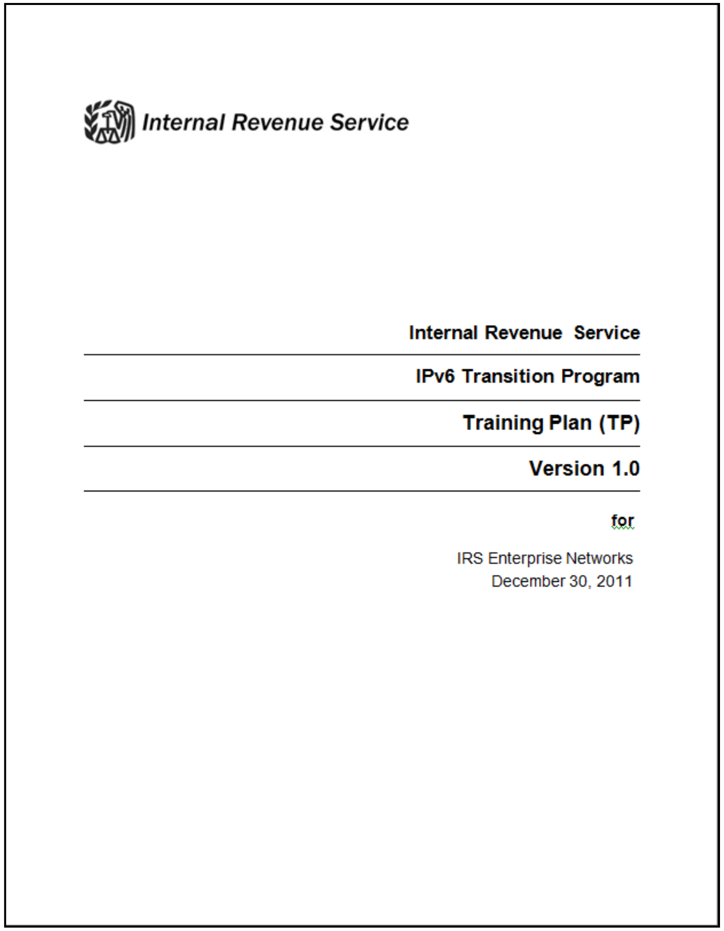
TO: See Distribution List

FROM: Barry E. Kearns
Director, Office of Procurement Policy

SUBJECT: **Compliance with Internet Protocol Version 6 (IPv6)**

1. **PURPOSE**. This Policy and Procedures Memorandum (P&P) sets forth the requirements for the review, inclusion, and compliance with IPv6 technology capabilities.
2. **SUMMARY OF LATEST CHANGES**: This P&P is an initial P&P and must be read in its entirety.
3. **EFFECTIVE PERIOD**: This P&P is effective upon issuance and remains in effect until superseded.
4. **SCOPE**: This policy applies to acquisitions that procure information technology (IT) equipment, i.e., hosts, routers, and network protection devices, as well as IT software and services, such as services by an Internet Service Provider (ISP) and a Managed Service Provider (MSP). IPv6 requirements apply to many electronic devices, to include mobile telephones, laptops, in-vehicle computers, televisions, cameras, building sensors, medical devices, etc.
5. **INTRODUCTION**: Computers and other devices use the IP to communicate over a network. Each network device requires a unique IP address. In early 2011, the Internet Cooperation for Assigned Names and Numbers (ICANN) assigned the last available pool of IP version 4 (IPv4) addresses. IPv6 replaces IPv4 and has an almost unlimited number of addresses. Some vendors have not implemented IPv6

Training



Internal Revenue Service

Internal Revenue Service

IPv6 Transition Program

Training Plan (TP)

Version 1.0

for

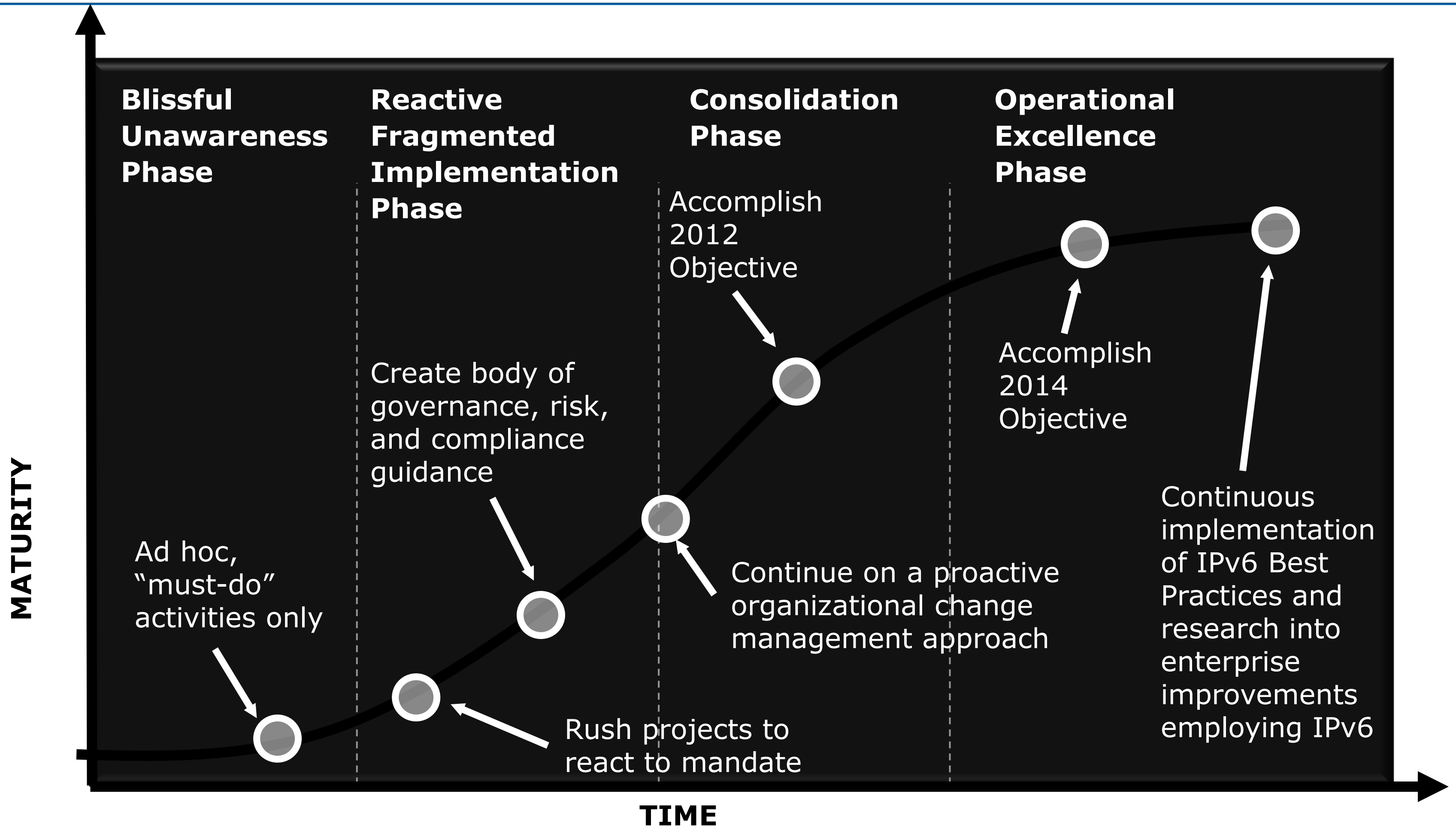
IRS Enterprise Networks
December 30, 2011

	Levels of Engagement				
Topic	1	2	3	Focus	Audience
Overview	x			Awareness	Executive, Master
Fundamentals, Design, and Deployment		x		Engineering	Master, Journeyman
Security Engineering			x	Engineering	Master, Journeyman
Application Developer			x	Engineering	Master, Journeyman
IT Acquisition		x		Operational	Master, Journeyman
Enterprise Architecture		x		Operational	Master, Journeyman
Service Desk (ITSM)		x	x	Operational	Journeyman, Apprentice
Change Management (ITSM)		x	x	Operational	Journeyman, Apprentice
Security Operations		x		Operational	Journeyman, Apprentice

A training “continuum” must be established for those personnel across the enterprise working in their respective functional areas who must know IPv6 at an apprentice, journeyman, and master level. The comparison is software engineering.

IRS

Training


Blissful Unawareness Phase
Reactive Fragmented Implementation Phase
Consolidation Phase
Operational Excellence Phase
Ad hoc, “must-do” activities only
Create body of governance, risk, and compliance guidance
Rush projects to react to mandate
Continue on a proactive organizational change management approach
Accomplish 2012 Objective
Accomplish 2014 Objective
Continuous implementation of IPv6 Best Practices and research into enterprise improvements employing IPv6
MATURITY
TIME

Result of a successful training plan: Transition PMO staff from Tiger Team to Project Mentoring role

Closing

1. Identification of strategic business objectives
2. Identification of transition priorities
3. Identification of transition activities
4. Transition milestones
5. Transition criteria for legacy, upgraded, and new capabilities
6. Means for adjudicating claims that an asset should not transition in prescribed timeframes
7. Technical strategy and selection of transition mechanisms to support IPv4/IPv6 interoperability
8. Management and assignment of resources for transition
9. Maintenance of interoperability and security during transition
10. Use of IPv6 standards and products
11. Support for IPv4 infrastructure during and after 2008 IPv6 network backbone deployment
12. Application migration (if required to support backbone transition)
13. Costs not covered by technology refresh
14. Transition governance
    - a. Policy
    - b. Roles and responsibilities
    - c. Management structure
    - d. Performance measurement
    - e. Reporting
15. Acquisition and procurement
16. Training
17. Testing

Questions?

Department of the Treasury
Internal Revenue Service
www.irs.gov