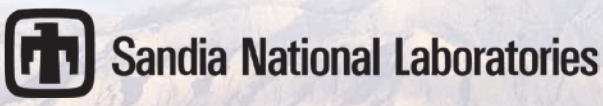
SANDIA REPORT
SAND2014-5032
Unlimited Release
Printed July 2014

Cyberspace Modernization: An Internet Protocol Planning Advisory

Curtis M. Keliiaa and Victor N. McLane

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2014-5032
Unlimited Release
Printed July 2014

Cyberspace Modernization: An Internet Protocol Planning Advisory

Curtis Keliiaa, Advanced Information & Network System Engineering
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1324

Victor McLane, Infrastructure Computing Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0838

Abstract

A common challenge across the communications and information technology (IT) sectors is **Internet + modernization + complexity + risk + cost**. Cyberspace modernization and cyber security risks, issues, and concerns impact service providers, their customers, and the industry at large. Public and private sectors are struggling to solve the problem. New service opportunities lie in mobile voice, video, and data, and machine-to-machine (M2M) information and communication technologies that are migrating not only to predominant Internet Protocol (IP) communications, but also concurrently integrating IP, version 4 (IPv4) and IP, version 6 (IPv6). With reference to the "Second Internet" and the "Internet of Things", next generation information services portend business survivability in the changing global market. The planning, architecture, and design information herein is intended to increase infrastructure preparedness, security, interoperability, resilience, and trust in the midst of such unprecedented change and opportunity.

This document is a product of Sandia National Laboratories Tribal Cyber and IPv6 project work. It is a Cyberspace Modernization objective advisory in support of bridging the digital divide through strategic partnership and an informed path forward.

ACKNOWLEDGMENTS

About the Authors
Curtis M. Keliiaa is a Senior Network Engineer with Sandia National Laboratories. He has a 35-year career history in the information and communications industry and has attained multiple operating system, networking, and cybersecurity industry certifications. Pertinent to this report, he is currently an ISC^2 Certified Information System Security Professional (CISSP), and an IPv6 Forum Gold Certified Engineer.

Victor N. McLane is a Computing Infrastructure Engineer with Sandia National Laboratories. He holds an MS Computer Science and is an IPv6 Forum Silver Certified Engineer.

Sandia National Laboratories Document Reviewers
Andjelka Kelic, and Barbara J. Jennings, Policy and Decision Analytics; Raymond C. Parks, Assurance Tech and Assessments; William D. Atkins, Security Systems Analysis; Kenneth A. Bernier, Telecom Infrastructure; Kevin S. Nauer, Cyber Security Technologies; Benjamin Mar, Trusted and Secure Systems; Richard D. Gay, Communication and Network Systems; Robert A. Mason, Network Design and Operations; Ron H. Mori, International Safeguards & Tech Systems; and Tim L. MacAlpine, Engineering Infrastructure

Sandia National Laboratories Tribal Cyber Project Management Team
Program Manager: Laurence E. Brown; Responsible Manager: Jeremy L. Banks; Primary Investigator: Curtis Keliiaa; Project Coordinator: Benjamin Mar

Acknowledgement of Contribution
Appreciation is extended to the membership of the Native American Telecom Association (NATA), the National Tribal Telecom Association (NTTA), the Arizona New Mexico Telecom Association (ANMTA), the Tribal Telecom Conference Advisory Council, the Sandia National Laboratories New Mexico Small Business Assistance program, the Fort Mojave Indian Tribe Department of Emergency Response, the Fort Mojave Police Department, and Fort Mojave Telecom, Inc. for collaboration in support of this work.

Appreciation is extended to all members of Sandia National Laboratories Resilient Infrastructure Protection and Trust Interdisciplinary Expertise (RIPTIDE) team for important contributions to the practice of cyberspace modernization.

Literature Review
The authors utilized the works of the National Institute of Standards and Technology (NIST), the Internet Engineering Task Force (IETF), the SysAdmin, Audit, Network, Security (SANS) Institute, the Rocky Mountain IPv6 Task Force, and the IPv6 Security: ISBN-13 978-1-58705594 text by Scott Hogg and Eric Vyncke, and the Deploying IPv6 Networks: ISBN-13-1-58705-210-5 text by Ciprian Popovicui, Eric Levy-Abegnoli, and Patrick Grossetete for literature review and reference supporting this work. Additional USG and industry references were also valuable and are noted within the text.

CONTENTS

FIGURES

TABLES

NOMENCLATURE

ANMTA	Arizona New Mexico Telecom Association
ARIN	American Registry for Internet Numbers
DOC	Department of Commerce
DOE	Department of Energy
DHS	Department of Homeland Security
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
ISC^2	International Information Systems Security Certification Consortium
NAv6TF	North American IPv6 Task Force
NATA	Native American Telecom Association
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
NTTA	National Tribal Telecom Association
RMv6TF	Rocky Mountain IPv6 Task Force
SANS	SysAdmin, Audit, Network, Security Institute
SNL	Sandia National Laboratories
USG	United States Government

CYBERSPACE MODERNIZATION EXECUTIVE SUMMARY

Cyberspace Modernization: Cyberspace modernization comprises emerging next-generation technology advancements in conjunction with continued dependence on waning legacy technologies. Decision makers are faced with a dilemma: When to invest in emerging technologies that will eventually eclipse older technologies. We note that although next generation technologies appear similar, they are fundamentally different than their legacy predecessors. We submit that the time for investment is now in large part due to the North American Internet protocol, version 4 (IPv4) address exhaustion event that is anticipated by February 2015 if not sooner. This imminent exhaustion event creates immediacy for investment in cyberspace modernization beginning with Internet protocol, version 6 (IPv6). Finally, we present that we are at a threshold of unprecedented technological change between legacy and next generation technologies that portends business survivability in the changing global market.

Economic Development: IPv6 value extends beyond its function as a network transport and the availability of more addresses. IPv6 comprises a suite of technologies that provide a foundation for new mobile device and mobile network services, and is the source of scalability for the Internet of Things. IPv4 simply cannot accommodate growth. Therefore economic development based on information and communication technologies innovation is dependent on IPv6.

Workforce Development: Subject matter expertise is the most substantial gap standing between legacy and next generation return on investment. Technology differences are significant and expertise with IPv4 does not imply expertise with IPv6. Building subject matter expertise starts with executive championship, without which change may be engaged in crisis without the luxury of deterministic planning for security, interoperability, resilience, and trust or realization of maximum return on investment. This is necessary to incentivize workforce development.

Risk Management: A phased approach and best practices are considered in this IP process and task guidance that includes full life cycle risk management for management, operational, and technical levels of risk. This guidance implies a progressive and iterative approach to risk management and combines likelihood of disruptive event/consequence and difficulty of adversarial attack/consequence analysis as valuable methods to garner probabilistic/quantitative and cyber/qualitative insight to risk management.

Security, Interoperability, Resilience, and Trust: Concept to disposition or full life-cycle consideration must be given to realize baked-in security, interoperability, resilience, and trust. We demonstrate a means to achieve these integrated capabilities with careful attention paid to As-Is, Transitional, and To-Be architectures or profiles with tested and measured progress toward dual stack (IPv4v6) enabled services.

Path Forward: The path forward is largely unchartered. We illustrate information service development guidance with primary consideration given to cybersecurity in the transition from legacy to next generation technologies. We expand the level of effort to include preparedness, security, interoperability, resilience, and trust in the midst of unprecedented change, vulnerability, threat, and opportunity.

1. INTRODUCTION

Next generation information assurance and protection involves several sets of emerging information and communication technology challenges. Emerging Internet Protocol (IP) and radio frequency (RF) communication standards are widening the divide between conventional or legacy and next generation technologies. This document presents a cyberspace modernization IP planning approach to assist in the architecture, design, and deployment of next generation technologies with respect to emerging standards, security, interoperability, resilience, trust, and integration requirements.

Planning for integration and the eventual and ubiquitous deployment of next generation technologies requires knowledge of IP version 6 [1] (IPv6) and associated Internet modernization technologies (i.e. broadband, mobility, cloud, and machine-to-machine (M2M) communications) in order to build a firm technical foundation for optimal deployment of new services. Experience must also be gained to address complex cybersecurity challenges. The next generation information assurance and protection approach considers a broad application of next generation technologies across diverse infrastructures that will become increasingly interconnected. (i.e. education, healthcare, emergency services, energy, agriculture, transportation).

The first Internet is built on legacy technologies originating in the 1960's and 70's with deployment that continues from the 1980's to today via IPv4. The first Internet gave raise to client/server and World-Wide-Web based information services. The "Second Internet" is being built on next generation technologies originating in the 1990's with deployment continuing into the foreseeable future via IPv6. The "Second Internet" is giving raise to mobility and network mobility (NEMO) with coupling to virtual system and cloud based information services. The "Internet of Things" is another aspect of next generation technologies. The "Internet of Things" is facilitated through M2M communications, which include potential self-organizing device and network deployments via IPv6.

This document is presented for planning in particular to an IP dual stack (IPv4v6) transition approach. Planning for Automated Tunneling, Network Address Translation (NAT), and Application Layer Gateways (ALG) transition mechanisms are not included in this document.

The value of planning with security, interoperability, resilience, and trust begins with an investment at the onset of a project or program. The return on investment will be brought forward by well-informed deployment of secure, resilient, and trusted advanced information services in the 21st century.

1.1. Justification

The IP address space was initially designed to use a 32-bit space, providing for 4.3 billion unique addresses. The Internet has grown beyond the capacity offered by 32-bit addressing. IPv6 expands the capacity of the Internet to 128-bit addressing. Internet service providers and enterprise organizations must enable IPv6 on internal and external facing networks to facilitate continued connectivity with the world at large. Expanding the availability of network addresses to the level afforded by IPv6 will facilitate creative new ways to process and share information.

The Internet Assigned Numbers Authority [2] (IANA) allocated the last available IPv4 allocations to the five regional Internet registries on February 3, 2011. The European and Asian regional Internet registries have reached post exhaustion of available IPv4 address allocations. The North American regional Internet registry, American Registry for Internet Numbers (ARIN), is in the final phase four (April 2014) with less than one remaining /8 IPv4 address allocation. ARIN post exhaustion is anticipated February 2015.

Solutions providers and operators face the challenge of converging legacy technologies and dependencies with emerging next generation technologies and dependencies. This guidance supports IPv6 planning to assist in the management and convergence of emergent next generation advanced information services.

1.2. Requirements

Two requirements [3] are to be considered throughout this document.

1. Cybersecurity is a design requirement. You'll note that Cybersecurity is task 14 in the process outlined in this document but is considered from initiation to disposition. Planning, architecture, design, and deployment activities must include cybersecurity as a design requirement in order to have security, resilience and trust "baked-in".

2. Interoperability is an operational requirement. It is expected that transition from IPv4 to IPv6 will result in dual stack dependence for most organizations for the foreseeable future. These two technology suites are not compatible as the total IPv4 address space is insignificant by comparison to IPv6.

1.3. Tenets of Cyberspace Modernization and Risk Mitigation

This document is written with consideration for several tenets of managed security.

1. Confidentiality of Communications
2. Integrity of Information
3. Availability of Services
4. System Security
5. Network Security
6. Device Security
7. Information Assurance
8. Resilience to Disruption of System Services and Service Dependencies
9. Trusted Systems for Fail-Secure Functionality
10. Non-Repudiation of Access to Sensitive Information
11. Provenance of Data Handling and Data Modification
12. Identity and Identity Credential Protection
13. Authorized Access
14. Authenticated and Appropriate Access
15. Defined Roles and Responsibilities
16. Separation of Duties
17. Known State of Operational Security
18. Continuous Monitoring
19. Authentication, Authorization, and Accounting (AAA)
20. Cyber Critical Infrastructure Protection (Cyber CIP)
21. Compliance with laws, regulations, and Constitutional requirements
22. Privacy and Civil Liberties involving collection, disclosure, or use of personal information
23. Agility and Adaptation to Technology Change
24. Training, Education, and Awareness
25. Informed Decisions

How to use this document: Questions should be developed to define organization specific goals, objectives, and requirements. The recommended approach is to conduct subject specific interviews pertaining to existing and emerging service and system implementations with attention paid to management, operational, and technical risks and concerns. The resulting dialog will inform the Initiation, Acquisition/Deployment, Implementation, Operations/Maintenance, and Disposition phases of cyberspace modernization efforts. Use what you find pertinent in this document and add what may be missing.

Information gathered including system and network diagrams may be **[INSERTED]** into this document as a means of recording the results of planning, investment decisions, and service, system, network, and security architectures and profiles for an organization. New content should be reviewed for sensitivity, categorization, and appropriate marking of information.

You will note that three types of architecture or profiles are referenced in this document: As-Is, Transitional, and To-Be. The end result should help the organization understand where it is, where it wants (or needs) to go, and how it is going to get there. The terms profile and architecture are used interchangeably to illustrate iterative and progressive planning and design where the transitional architecture bridges the As-Is and To-Be architectures.

1.4. Project Perspectives

Understanding the perspectives of decision makers, acquisition/deployment and operations/maintenance personnel, and system users are important to the successful outcome of complex cyberspace modernization efforts. Requirements elicitation and communication of project goals and objectives are essential to meet user expectations. Provided below are example questions that provide initial information gathering prior to formal project requirements elicitation:

Heilmeier's Catechism[1]

1. What are you trying to do? Articulate your objectives using absolutely no jargon.
2. How is it done today, and what are the limits of current practice?
3. What's new in your approach and why do you think it will be successful?
4. Who cares? If you're successful, what difference will it make?
5. What are the risks and the payoffs?
6. How much will it cost? How long will it take?
7. What are the midterm and final "exams" to check for success?

Personnel Observations[2]

1. What is your role or responsibility?
2. Is there someone else who can back you up in your absence?
    a. Can you give me their name?
3. Describe your responsibility or duties.
4. Are there procedures or protocols written for these duties?
    a. How do you access them, computer? Written?
5. Is training provided for you to do your job?
    a. What type?
6. Can you give an example or tell me about a scenario of doing your job?
7. What went well?
8. Did anything not go well or as intended?
    a. Why?
9. Is it possible that this could occur again?
10. In a perfect world what would you change?
11. Is there anything else that you need you to do your job better?
12. Is there anything else that I have missed or that you want to share?

[1] http://cseweb.ucsd.edu/~ddahlstr/misc/heilmeier.html (George H. Heilmeier 5/22/1936-4/21/2014)
[2] B. Jennings, Sandia National Laboratories

2. NEXT GENERATION ADVANCED INFORMATION SERVICES

This next generation advanced information service development guidance describes technical phase processes and high-level tasks for deployment of dual stack IP (IPv4v6). IPv6 deployment includes five phases [4]: Initiation, Acquisition/Deployment, Implementation, Operations/ Maintenance, and Disposition. Plan tasks represent a path forward for IPv6 planning and deployment[3] through this phased approach.

2.1. Initiation

The initiation phase is concerned with understanding existing infrastructure investments to prepare for technology change (priorities and scope). It is important for an organization to understand its current environment before deploying IPv6 in order to orient work with goals objectives, and requirements. By understanding the current environment an appropriate transition approach can be determined for an organization while adhering to best practices to ensure relative parity between IPv4 and IPv6 operations. Inventories should be established and maintained for long-term operations and security benefit.

"Baking in" security, resilience and trust starts here.

Task 1 – Develop Baseline IPv6 Knowledge
Activity: Work force development with recommended technical references and training
Objective: Establish baseline IPv6 knowledge, skills and abilities equivalent to existing IPv4 level of expertise

- Organizational training, education, and awareness program
- College and University degree programs
- Conferences
- Industry training and certification programs
- Self-study
- Other

Suggested self study: Deploying IPv6 Networks [5]: ISBN-1587052105 and IPv6 Security [6]: ISBN-13 978-1-58705594

[INSERT ORGANIZATION SPECIFIC TRAINING PLAN HERE]

Task 2 – Hardware Inventory
Activity: Understand current hardware investments
Objective: Establish baseline for existing and approved hardware

- Mobile devices
- Computing platforms
- Network devices
- Other

[INSERT HARDWARE INVENTORY RESULTS HERE]

[3] Information sources include Deploying IPv6 Networks: ISBN-1587052105

Task 3 – Software Inventory
Activity: Understand current software and application investments
Objective: Establish baseline for existing and approved software and applications

- Operating Systems
- Applications
- Service Delivery (middleware)
- Other

[INSERT SOFTWARE INVENTORY RESULTS HERE]

Task 4 – Service Inventory
Activity: Understand current customer service investments
Objective: Establish baseline IPv4 based customer services

- Hosting/Content Delivery
- Telecommunications
- VoIP
- Software as a Service (SaaS)
- Desktop as a Service (DaaS)
- Platform as a Service (Paas)
- Infrastructure as a Service (IaaS)
- Multimedia
- Mobility
- Mobile Networks
- Other

[INSERT SERVICE INVENTORY RESULTS HERE]

Task 5 – Operational Support Tools Inventory

Activity: Understand current operational support and network management investments

Objective: Establish baseline IPv4 operational support and network management dependencies

- Network Monitoring (Network Operations Center)
- Detection, Alarm, and Notification (Systems Operations Center)
- Other

[INSERT OPERATIONAL SUPPORT TOOLS INVENTORY RESULTS HERE]

Task 6 – Cybersecurity Tools Inventory

Activity: Understand current cybersecurity tools investments

Objective: Establish baseline IPv4 cybersecurity posture

- Perimeter Security (firewalls, access control lists (ACL), proxy/Application Layer Gateway (ALG), Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)/Data Loss Prevention (DLP)/Anti-Virus (AV)
- Systems Security (permissions, privileged accounts, policies)
- Telecommunications Security (tunneling, IP Security (IPSec), Internet Key Exchange (IKE), IEEE 802.1AE (MACsec), Layer 2 (L2) and Layer 3 (L3) access controls, Secure Socket Layer (SSL)/Transport Layer Security (TLS)
- Operations Security (outage schedules, high availability, backup/restore, IT disaster recovery (ITDR) planning, continuity of operations planning (COOP)
- Other

[INSERT CYBERSECURITY TOOLS INVENTORY RESULTS HERE]
[INSERT AS-IS ARCHITECTURE/PROFILE RESULTS HERE]

2.2. Acquisition/Deployment

The acquisition and development phase is concerned with taking the information gathered during the initiation phase, conducting requirements elicitation, and developing a set of IPv6 deployment architectures (Service, System, Network, Security). The acquisition/development phase will work with the three types of architecture or profiles: As-Is, Transitional, and To-Be, where the transitional architecture/profile bridges the As-Is and To-Be architectures.

Requirements Elicitation: Requirements elicitation is essential to guide investment strategy, provide a transparent user experience, and to eliminate disruption during modernization activities. A useful approach is to conduct site visits and stakeholder and operator interviews followed by briefings in an iterative dialog until agreement on goals and objectives is reached. Secondly, a series of infrastructure surveys to identify assets, systems and networks would be useful to determine operational functions, dependencies, and priorities. This information would then inform risk assessment and mitigation prioritization activities. Below is an illustration of how these processes align with National Infrastructure Protection Plan [7] (NIPP) guidance.

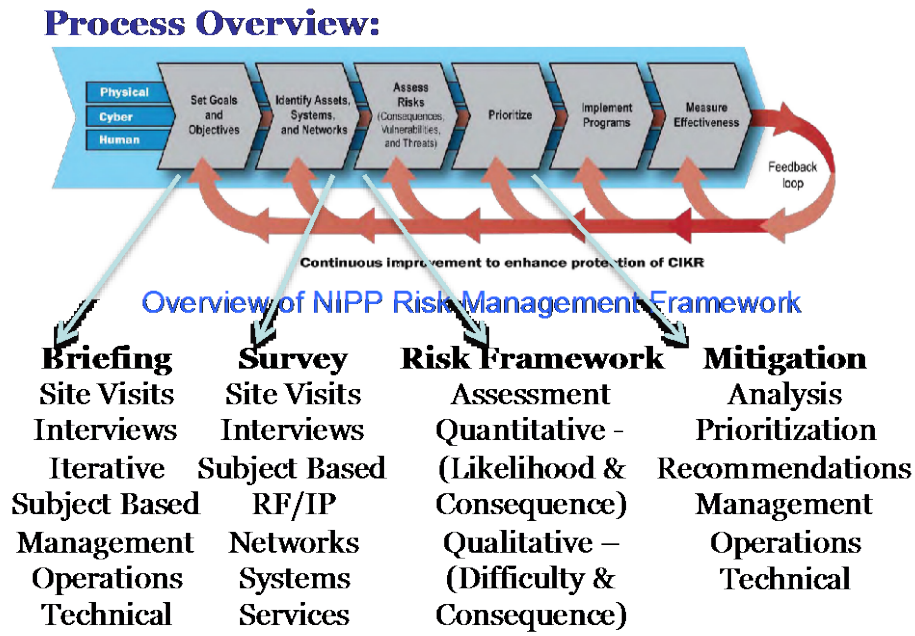


Figure 1 National Infrastructure Protection Plan Process Alignment

Baseline or high-level requirements within the context of this document include:

1. Risk Management – Organizational mitigation of management, operational, and technical risks
2. Training – Workforce development to build requisite subject matter expertise
3. Cybersecurity – Information asset protection policy and security comprising confidentiality, availability, and integrity mechanisms
4. Interoperability – Capability to operate with concurrent legacy and next generation technologies
5. Change Management – Management of continual change and evolution of information services
6. Patch Management – Means to deploy software updates to applications, systems, and networks
7. Configuration Management - Management of ongoing configuration change to information assets
8. Continuous Monitoring – To detect anomalous activity, unauthorized hardware and software, and verify protection mechanisms function as designed and implemented

[INSERT BRIEFING GOALS, OBJECTIVES, AND REQUIREMENTS HERE]
[INSERT ASSET, SYSTEMS, AND NETWORKS SURVEY RESULTS HERE]

Task 7 – Information Service Planning

Activity: Conduct requirements elicitation to understand IPv6 customer service investments.
Objective: Establish an information service planning baseline for IPv6 enabled services.
Information service architecture example: Rural Internet service provider (ISP)/Telecom:

Internal Business Areas:

1. Human Resources
2. Billing and Finance
3. Business Planning
4. Policy and Legal
5. Network Operations
6. Computing
7. Cybersecurity
8. Business Development and Marketing
9. Customer Services and Support
10. Administration
11. Other

IPv6 Service Base:

1. Internet Access
2. Telephony
3. Broadband
4. Cellular/LTE
5. VoIP
6. Multicast/PIM-SM
7. Video Streaming
8. Data Hosting – Data Center/Virtualization
9. Cloud Computing
10. SaaS, Daas, PaaS, IaaS
11. Data Storage - SAN
12. Common Core Services (DNS, DHCP, NTP, LDAP, SIP, IPAM)
13. Identity and Access Management (ICAM)
14. Content Delivery
15. Mobility
16. NEMO
17. Cybersecurity Services and Performance Monitoring
18. Essential Function 2: Communications High Availability/Alternate Path
19. Email
20. Web Hosting
21. Quality of Service (QoS) and Service Level Agreements (SLA)
22. Tele-Medicine
23. Utilities
24. Critical Infrastructure Sector Control Systems
25. 911 Service
26. Enhanced 911 (E911)
27. Next Generation 9-1-1 (NG9-1-1)
28. (ITDR) Alternate Data Center/Work Site
29. Other

30. **Customer Base**:

1. Rural Subscribers
2. Rural Businesses
3. Municipal Subscribers
4. Municipal Businesses
5. Inter-State Subscribers
6. Inter-State Businesses
7. Emergency Response
8. Public Safety Answering Points (PSAP)
9. Information Sharing & Analysis Centers (ISAC)
10. Anchor Institutions – Government
11. Anchor Institutions – Health
12. Anchor Institutions – Law Enforcement
13. Anchor Institutions – Education
14. Science & Engineering – Industry
15. Oil and Gas
16. Energy Grid
17. Finance
18. Service Providers (ISP, PSTN, Telecom, Datacenter)
19. Transportation
20. Manufacturing
21. Water/Dams
22. Agriculture
23. Residential Smart Home
24. Other

Task 8 – IPv6 Numbering Plan

Activity: Obtain assigned IPv6 address space and develop a numbering/addressing plan.
https://www.arin.net/

Objective: Establish a baseline IPv6 numbering schema, develop an IPv6 over IPv4 address overlay where necessary, and plan for dual stack IP address management (IPAM).

Site prefix note: The addressing scheme in this document assumes an ISP prefix of 32 bits. Prefix 2001:DB8::/32 is used for examples in this document.

Prefix length note: With the exception of loopback addresses and point-to-point (PTP) links between routers, all subnet prefixes are 64 bits. Leading zeros in 16 bit Hexadecimal notation between colons can be dropped and a series of zeroes can be concatenated (once only) with "::".

How might the service planning in step 7 map to an IPv6 number plan?

Network prefix /32	**External 0000 /36**	**Customer Subnets /52 (16 bits = 65535 (64K)**	**Per Service Subnets /64 (12 bits = 4096)**	**Interface Identifier /128**
2001:DB8::/32	0000	0x1 (Existing Customer Subnets 2200 + up to 4096, with overlay?)	0x1 (Existing v4 overlay needed? Decimal 1 - 255 = 0x1 - 0xFF for Class C)	ABCDDEFFFEADBEEF (EUI 64 example)
2001:DB8::/32	0000	0x1	0x2	::1
2001:DB8::/32	0000	0x1	0x3	::2
2001:DB8::/32	0000	0x1	0x4	::3
2001:DB8::/32	0000	0x1	0x5	::4
2001:DB8::/32	0000	0x1	0x6	A::1
2001:DB8::/32	0000	0x1	0x7	B::2
2001:DB8::/32	0000	0x1	0x8	C::3
2001:DB8::/32	0000	0x1	0x9	FFFF::FF01
2001:DB8::/32	0000	0x1	0xA	…
2001:DB8::/32	0000	0x1	…	…
2001:DB8::/32	0000	0x1	0xFF (Class C overlay 8 bits for 255 hosts)	…
2001:DB8::/32	0000	0x1	0x100 (New IPv6 Subnet growth > 255)	…
2001:DB8::/32	0000	0x1	…	…
2001:DB8::/32	0000	…	…	…
2001:DB8::/32	0000	0xFFF	0xFFF	…
2001:DB8::/32	0000	0x1000 (New Customer Subnets > 4096	0x0 (restart service subnet numbering)	…
2001:DB8::/32	0000	…	…	…
2001:DB8::/32	0000	0xFFFF	0xFFF	…

Table 1 IPv6 External Network Prefix Breakout

Internal service numbering example:

Network prefix /32	Internal 0001 /36	Business Area Subnets /52 (16 bits = 65535 (64K)	Per Business Area Subnets /64 12 bits = 4096 (4K))	Interface Identifier /128
2001:DB8::/32	0001	0x1 (Existing v4 overlay needed? Decimal 1 - 255 = 0x1 - 0xFF for Class C)	0x1 (Existing v4 overlay needed? Decimal 1 - 255 = 0x1 - 0xFF for Class C)	ABCDDEFFFEADBEEF (EUI 64 example)
2001:DB8::/32	0001	0x2	0x2	::1
2001:DB8::/32	0001	0x3	0x3	::2
2001:DB8::/32	0001	0x4	0x4	::3
2001:DB8::/32	0001	0x5	0x5	::4
2001:DB8::/32	0001	0x6	0x6	A::1
2001:DB8::/32	0001	0x7	0x7	B::2
2001:DB8::/32	0001	0x8	0x8	C::3
2001:DB8::/32	0001	0x9	0x9	FFFF::FF01
2001:DB8::/32	0001	0xA	0xA	…
2001:DB8::/32	0001	0xB	0xB	…
2001:DB8::/32	0001	0xC	0xC	…
2001:DB8::/32	0001	0xD	0xD	…
2001:DB8::/32	0001	0xE	0xE	…
2001:DB8::/32	0001	0xF	0xF	…
2001:DB8::/32	0001	0x10	0x10	…
2001:DB8::/32	0001	…	…	…
2001:DB8::/32	0001	0xFFFF	0xFFF	…

Table 2 IPv6 Internal Network Prefix Breakout

What are the benefits of this IP address schema?
This schema considers market development and information separation such as customer information from internal business information. It considers a consistent IPv6 overlay with IPv4 deployment that facilitates dual stack hosts that may communicate over either IP version. A consistent IPv4v6 address schema also aids network management where a host may be managed over IPv4 but communicate over IPv6.

What are the drawbacks of this schema?
Business needs or investment posture change over time. An IP address schema should be flexible to accommodate changes over time. This schema was designed with this in mind, although unforeseen circumstances may require a redesign in the future.

It is important to note some of the fundamental differences between IPv4 and IPv6 of particular importance to address use and planning. An IPv4 node typically has one address unless it is multihomed. IPv4 relies on broadcast for data link layer (layer 2) media access control (MAC) address to network layer (layer 3) IP address resolution via the address resolution protocol (ARP). IPv4 32 bit addresses are much more restrictive than IPv6 128 bit addresses.

IPv6 comprises multiple address types that permit link local (same subnet), local (same organization different subnet), and global (globally Internet routable) connectivity. Therefore a single IPv6 interface will have multiple IPv6 addresses and address types. IPv6 relies on multicast for data link layer MAC address to IP address resolution through the neighbor discovery protocol (NDP) [8]. IPv6 addressing is more flexible but adds complexity that must be managed.

For example, IPv6 address types per interface include:

- Loopback address
- Link local addresses
- Unicast or anycast (if configured)
- Unique local addresses (ULA) or Site local (depreciated)
- Multicast addresses (all nodes, all routers, multicast services, etc.)
- Subnet router anycast address
- Stateless Address Auto-Configuration (SLAAC) using Extended Unique Identifier on 64 bits (EUI-64) addresses
- Privacy extension addresses using Cryptographically Generated Addresses (CGA) or randomly generated addresses

Fixed addressing note: Servers and other hosts requiring fixed addressing may be assigned fixed IPv6 addresses assigned for their exclusive use. Anticipate for the foreseeable future that each such host will operate in a dual-stack IPv4v6 environment, the host's IPv4 address may be used in the formation of its IPv6 address.

Dynamic addressing note: Alternatively dynamic addressing may be used. The two primary methods for dynamic configuration of IPv6 hosts are Dynamic Host Configuration Protocol for IPv6 (DHCPv6) and the IPv6 IETF SLAAC standard [9]. DHCPv6 is easier to centrally manage within an enterprise, includes the provision of IPv6 addresses of DNS servers, and provides a built-in mechanism for dynamic population of IPv6 DNS zones for reverse name resolution.

IP Address Management (IPAM): IPAM for IPv6 and IPv4 addressing is necessary to track IP address assignments and in many cases inventory with an IP address as a key identifier. Additionally network connections and disconnects may be associated to validated IP addresses. IPAM may use a new database or an existing inventory database may be modified.

[INSERT ORGANIZATION SPECIFIC IP NUMBERING PLAN HERE]
[INSERT IP SERVICE PLANS HERE]
[INSERT SERVICE AND SYSTEM TRANSITIONAL AND TO-BE ARCHITECTURES/ PROFILES HERE]

Task 9 – Develop an IPv6 Test Plan
Activity: Establish an IPv6 test plan that includes dual stack planning, functionality, operations, and security.
Objective: Preparation for deployment of external customer facing services before internal facing services.

The test plan will consist of the following recommended activities:

- Incorporate training requirements
- Assess access layer deployment options
- Assess network edge, distribution and core deployment options
- Assess system datacenter, desktop and operational support system (OSS) deployment options
- Plan device (router) configuration specifics
- Plan system configuration specifics
- Test fixed network device and system configurations
- Test fixed network device and system functionality and performance
- Test fixed network device and system security
- Test mobile network device and system configurations
- Test mobile network device and system functionality and performance
- Test mobile network device and system security
- Test service application functionality and performance
- Test service application security
- Review any other identified activities required to meet customer needs and approve results for implementation
- Enable configurations on network devices and systems
- Deploy services and applications

[INSERT ORGANIZATION SPECIFIC IP TEST PLAN HERE]

Task 10 – Infrastructure and Service Operations Upgrade Plan
Activity: Conduct infrastructure service, systems, network, security requirements elicitation to understand IPv4 existing infrastructure and integration of IPv6 (dual stack) on routers, switches, (VPNs, access layer, routing and routed protocols, network management, etc.), systems (servers, desktop, virtual, OSS), and security (cybersecurity, intrusion detection/prevention (IDS, IPS, DLP), patch management, monitoring)
Objective: Ensure systems and networks are capable of IPv6 and IPv4 dual stack functionality. Deploy external public-facing services [10] before internal services. Recommended external public-facing services are DNS, Email, and Web.

- Service Architecture Considerations
    - Training
    - External Public Facing/Internal Services
    - Fixed (Datacenter/Desktop)
    - Interoperability
    - Mobility [11] [12] [13] [14] (Mobile IP version 6 (MIPv6))
        - Home Agent (HA)
        - Home Agent Controller (HAC)
        - Mobile Node (MN)
        - Correspondent Node (CN)
    - NEMO (Arial, Terrestrial, Nautical)

    - Long Term Evolution (LTE) Advanced
    - Evolved-Universal Radio Access Network [15] (E-UTRAN)
    - ITDR/COOP
    - Change Management
    - Other
- System Architecture Considerations
    - Training
    - Client/Server [16] [17] [18], Virtualization, Clients/Desktop
    - Mobility
    - OSS
    - Computing Platforms
    - Applications
    - Patch Management
    - Other
- Network Architecture Considerations
    - Training
    - Mobile, Access, Distribution/Edge, Core [19] [20] [21]
    - Routed and Routing Protocols (Border Gateway Protocol (BGP), Interior Gateway Protocols (IGP), IP)
    - Access Layer (Multi-Protocol Label Switching (MPLS), Asynchronous Transfer Mode (ATM), Frame, Dialup)
    - VPN, Tunneling, Remote Access
    - Network Management/Monitoring
        - Common Core Services (DNS, NTP, DHCP, LDAP, SIP, IPAM, ICAM)
        - IPv4v6 Relative Functional Parity
    - Configuration Management
    - Other
- Cybersecurity Architecture Considerations
    - Training and Risk Management
    - Confidentiality, Integrity, Availability
    - Mobile, Access, Distribution/Edge, Core
    - Information Categorization and Protection (at rest and in transit)
    - Encryption (IPSec/IKE/TLS)
    - Tools (IDS, IPS, DLP, AV, Logging)
    - Incident Response (IR), Investigation and Evidence Handling
    - IPv4v6 Relative Security Parity
    - Continuous Monitoring
    - Other

Task 11 – Internal Network Upgrade Plan

Activity: Conduct systems and OSS requirements elicitation to derive IPv6 over IPv4 infrastructure (overlay) dependencies with operating systems, billing and accounting systems, Human Resources, etc. Note that cybersecurity must be considered.

Objective: Ensure internal services are capable of both IPv6 and IPv4 dual stack functionality.

- Internal Network Considerations
  - Training requirements for essential personnel
  - Operating System requirements
  - Database dependencies (middleware)
  - IPv4 backend communication dependencies (backups, automated job processing)
  - Critical system dependencies (Human Resources, Billing, Incident Response)
  - Cybersecurity [22]
  - Other

[INSERT NETWORK TRANSITIONAL AND TO-BE ARCHITECTURES/ PROFILES HERE]

Task 12 – Cost Analysis

Activity: Understand IPv4v6 (dual stack) implementation costs based on defined requirements [23].

Objective: Ensure upgrade from existing infrastructure to IPv6 enabled infrastructure costs and schedule meet business needs [24] and resources.

- Training, Education, & Awareness
- Network Infrastructure and Services (network gear)
- Computing Platforms and Critical Applications (servers, desktop, virtualization, OSS)
- IT Disaster Recovery (hot-site, warm-site, cold-site, virtual and cloud based-disaster recovery systems)
- Customer Services (Internet access, telephony, VoIP, etc.)
- Cybersecurity (monitoring, visibility and IDS/IPS/DLP for IPv4 only, Dual Stack, IPv6 only)
- Network Interconnectivity (interconnects, downstream and upstream ISP's)
- COOP
- Business Continuity Planning (BCP)
- Other

[INSERT ORGANIZATION SPECIFIC COST MANAGEMENT PLAN HERE]

2.3. Implementation

The implementation phase involves the secure installation and configuration of IPv6 equipment, tunnels, and translation mechanisms. The deployment stage differs depending on which deployment scenario is used (IPv6 pervasive deployment or IPv6 sparse deployment).

Task 13 – Build an IPv6 Test Bed

Activity: Evaluate IPv6 connectivity and IPv6 enabled network services. Become familiar with firewall and ACL rules for IPv6 (see the IPv6 Assessment of Next Generation Assurance & Protection section at the end of this document).
Objective: Development of a test environment to evaluate IPv6 technologies and services.
Outcomes: Familiarization with configuration of routing and routed protocols, IPv6 addressing, and functionality for co-existing IPv4 and IPv6 networks.
Depends upon: ACL rules, IPv6 numbering plan, and network device configuration.

Activities consist of the following:

- Establish network device configurations
- Develop a process for managing IPv6 enabled hosts
- Evaluate implementation options for IPv6 deployment
- Evaluate application of IPv4 firewall rule principles for IPv6 firewall rule implementation
- Enable and configure network devices and ACL rules for IPv6
- Verify firewall rules
- Test network and server configurations in the test bed for eventual deployment in the DMZ
- Review any other identified activities required to meet customer needs and approve results for implementation

Task 14 – Cybersecurity

Activity: Enable cybersecurity tools for monitoring and intrusion detection in dual stack environments. Perform cyber risk assessments for individual security functions and IR for IPv6 as a whole.
Objective: Monitor both IPv4 and IPv6 traffic and provide IR and recovery processes.
Outcomes: Secure IPv6 traffic in tandem with IPv4 traffic. IPv4 best practices may be applied to defending IPv6 networks. Cybersecurity tools will need to be assessed for dual stack protection as well as IPv6 related risks assessed.

Key activities are:

- Risk Assessment
  Risk assessment (RA) provides the initial foundation for evaluating the what, where, and why of needed protections for information systems and networks. NIST provides the basis for implementation of appropriate mitigations and cyber security of federal information system with NIST SP 800-53 [25], (Rev.4 April 2013). Next generation information assurance and protection includes cybersecurity as a design requirement to meet RA and System and Communications Protection (SC) security controls.

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Table 3 NIST SP 800-53 Security Control Identifiers and Family Names

The SysAdmin, Audit, Network, Security (SANS) Institute provides best practices guidance for cybersecurity in the form of 20 critical security controls [26]. The controls have also been mapped to NIST SP 800-53 [27] and are included within this document.

- Two risk assessment [28] approaches may prove useful:
  - Quantitative or probabilistic risk assessment (PRA) comprises likelihood and consequence to identify and mitigate management, operational, and technical event risks
  - Risk-informed management of enterprise security (RIMES) and qualitative risk assessment (QRA) comprises difficulty of attack and consequence to identify and mitigate management, operational, and technical adversarial risks
- Develop heat maps indicating unmitigated (inherent) risk and mitigated (residual) risk
- Consider risk management and threats appropriate to the organization, its mission, and operations. Considerations could include asset (what), threat agent (who), threat vector (how), rate of occurrence (when), and consequence of loss (cost). Threats may be considered on several levels, for example, adversarial outside threat agent or insider, social engineering or physical kinetic attack, technical compromise or natural disaster.
- Evaluate cybersecurity tools capability and gaps, for example IDS/IPS/DLP:
- Identify potential threats
- Modify, develop, or procure detection tools
- Update intrusion/incident response processes and procedures to accommodate IPv6 related events
- Integrate IPv6 into IR and recovery processes
- Evaluate configuration changes
- Perform continuous monitoring
- Other activities as necessary for the customer environment

Another consideration is Cyber CIP [29], which is addressed by a February 12, 2014 NIST Framework for Improving Critical Infrastructure Cybersecurity [30]. The framework comprises core Identify, Protect, Detect, Respond, and Recover activities, cybersecurity risk management maturity tiers including partial, risk-informed, repeatable, and adaptive, and function, category, and business requirement profiles. The framework helps organizations to understand the current level of cybersecurity sophistication and define a path to an improved critical infrastructure security posture.

[INSERT ORGANIZATION SPECIFIC PRA RISK ASSESSMENT HERE]
[INSERT ORGANIZATION SPECIFIC QRA RISK ASSESSMENT HERE]
[INSERT SECURITY TRANSITIONAL AND TO-BE ARCHITECTURES/ PROFILES HERE]

Task 15 – Update Firewalls for IPv6

Activity: Implement IPv6 firewall rules to maintain relative parity with IPv4 functionality and protection.

Objective: Firewalls protect networks after IPv6 is enabled while continuing to protect IPv4 traffic.

Outcome: Users will be able to utilize their IPv6 addresses to access Internet resources while the networks continue to be protected through firewall rules.

The key activities will be replicated for DNS, mail, WWW, and other services/applications

Key activities for each type of service are:

- Replicate IPv4 rules and exemptions for IPv6
- Document rules
- Test configurations
- Test functionality
- Test security
- Verify firewall rules
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy Firewalls

Task 16 – Enable DMZ for IPv6

Activity: Enable IPv6 connectivity on an external facing (customer and public) DMZ network environment. Establish firewall and ACL rules for IPv6. Prepare for IPv4 and IPv6 dual stack operations.

Objective: Ensure DMZ network services are enabled for IPv6 and IPv4 customer and public facing services.

Outcomes: External devices routing IPv4 and IPv6 packets for publically available services. Internal devices can route IPv4 and IPv6 packets. Devices recognize which hosts are IPv6 capable and can select the appropriate version of IP for routing packets.

Depends upon: Firewall and ACL rules to segment and protect internal network infrastructure from external customer and public facing services, IPv6 and IPv4 addressing overlay for dual stack systems, and network device configuration.

Activities consist of the following:

- Establish network device configurations
- Evaluate dependencies
- Dual stack addressing of IPv4/IPv6 enabled hosts.
- Enable and configure network devices and ACL rules for IPv6.
- Verify firewall rules
- Test configurations
- Test functionality
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy DMZ configuration options for IPv6

Task 17 – Enable External DNS for IPv6

Activity: Enable IPv6 connectivity on external DNS servers. Establish firewall and ACL rules for IPv6. Prepare DNS servers to resolve IPv6 addresses for named hosts.
Objective: Ensure DNS services are enabled for AAAA IPv6 and A IPv4 name records.
Outcomes: External devices routing IPv6 addresses can find publically available servers. Internal devices can resolve IPv6 addresses. Devices recognize which hosts are IPv6 capable and can select the appropriate version of IP for routing packets.
Depends upon: Firewall rules must allow communication between DNS servers.

Activities consist of the following:

- Establish DNS server in the test bed for eventual deployment in the DMZ
- Evaluate dependencies
- Develop process for registering records corresponding to IPv6 enabled hosts
- Enable and configure DNS for IPv6
- Verify firewall rules
- Test configurations
- Test functionality
- Test security
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy DMZ DNS

Task 18 – Enable External WWW for IPv6

Activity: Enable IPv6 connectivity on external facing WWW servers.
Objective: Ensure external hosts can access public web servers from both IPv4 and IPv6 addresses.
Outcomes: External devices routing IPv6 addresses can access publically available servers.

Activities consist of the following:

- Establish WWW server in the test bed for eventual deployment in the DMZ
- Evaluate dependencies
- Enable and configure WWW for IPv6
- Verify firewall rules
- Test configurations
- Test functionality
- Test security
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy DMZ WWW service

Task 19 – Enable External Email for IPv6

Activity: Enable IPv6 for external email services for incoming email connections.
Objective: Enable exchange of email messages with IPv6.
Outcomes: Able to send and receive emails to both external IPv4 and IPv6 mail servers.

Activities consist of the following:

- Establish email server in the test bed for eventual deployment in the DMZ
- Evaluate dependencies
- Configure mail servers for IPv6
- Verify Mail Transfer Agent (MTA) functionality
- Verify firewall rules
- Verify email connectivity
- Test configurations
- Test functionality
- Test security
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy DMZ email

Task 20 – Enable Other Outbound Services and Applications for IPv6

Activity: Enable IPv6 for external services, such as VoIP, remote-access, mobility.
Objective: Enable other network services to interact with IPv6 outside systems.

Activities consist of the following:

- Establish external service server in the test bed for eventual deployment in the DMZ
- Evaluate dependencies
- Identify relevant services and target devices for customer services (SLA and QoS)
- Develop IPv6 customer services
- Integrate IPv6 customer facing services
- Integrate IPv6 Overlay with IPv4 topology
- Test configurations
- Test functionality
- Test security
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy external service

Task 21 – Enable Internal Services and Applications for IPv4v6

Activity: Enable IPv6 for internal network and computing services. Internal service transition should follow external service transition for two reasons: 1) Knowledge and experience will be gained in a lower risk DMZ environment 2) Internal service transition with business critical services is expected to add complexity in which high-level expertise will be required to manage growth and change.

Objective: Enable other network services to interact with IPv6 systems.

Activities consist of the following:

- Establish internal service servers in the test bed for eventual deployment in internal networks
- Evaluate dependencies
- Integrate IPv6 Overlay with IPv4 topology.
- Identify relevant services and target devices for internal services.
- Test configurations
- Test functionality
- Test security
- Migrate subnets to the IPv6. Iterate sub-tasks for each sub-net.
- Interface with Active Directory site and LDAP services
- Interface with IPAM, DNS, and DCHPv6 services
- Calculate subnet addresses
- Enable subnet gateway
- Verify firewall rules
- Enable subnet nodes
- Integrate IPv6 into the Data Center Environment
- Client Server
- Virtualization/Cloud
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy internal service

[INSERT ORGANIZATION SPECIFIC UPDATED AS-IS ARCHITECTURES/ PROFILES HERE]

2.4. Operations/Maintenance

The operations phase often begins concurrently with the implementation phase. During operations, the focus is the secure operation of a dual stack or mixed IPv6/IPv4 environment. One of the most difficult challenges facing the operations staff in a mixed IPv6/IPv4 environment is keeping the two environments synchronized.

Task 22 – Upgrade IP Address Management for IPv4v6

Activity: Upgrade IPAM for dual stack. This may include changes to assess management, network management, and access controls databases and to scripts used for network configuration and IPAM.

Objective: IPv6 data is correctly recorded in an IPAM database. Functions dependent on IPAM (i.e. inventory, network access control, disconnects) still operate correctly with IPv4v6 systems.

Outcome: Have complete, reliable data in the IPAM system. Operations continue to fulfill the same functions in a dual stack environment as in an IPv4 only environment.

Key activities are:

- Establish IPAM service servers in the test bed for eventual enterprise deployment
- Evaluate dependencies
- Modify the IPAM database schema to include IPv6 data, including IPv6 addresses, link local addresses, subnet, network, DUID (DHCP unique identifiers)
- Modify or develop scripts for managing network devices
- Test configurations
- Test functionality
- Test security
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy IPAM service

Task 23 – Enable Active Directory or LDAP and ICAM Services

Activity: Enable Active Directory or Lightweight Directory Access Protocol (LDAP) controllers for dual stack (i.e. sites, DirectAccess).

Objective: Manage identity credential and access management (ICAM) service capability (Kerberos, Public Key Infrastructure (PKI)) associated with Active Directory/LDAP on IPv6 enabled systems. Outcome: Enabling IPv6 transparent to management of Active Directory/LDAP and ICAM systems.

Key activities are:

- Establish LDAP/ICAM service servers in the test bed for eventual enterprise deployment
- Evaluate dependencies
- Map IPv6 network over IPv4 network
- Configure sites, services on domain controllers
- Configure LDAP/ICAM services
- Test configurations
- Test functionality
- Test security
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy LDAP/ICAM services

Task 24 – Develop Systems Management for IPv4v6
Activity: Modify and deploy dual stack for supported operating systems.
Objective: Deploy standardized configuration for IPv6/dual stack.
Outcome: End user systems will be correctly configured for dual stack addressing. Systems will utilize correct policies and protections.

Key activities are:

- Establish Desktop (fixed, mobile, virtual desktop (VDT)) service servers in the test bed for eventual enterprise deployment
- Evaluate dependencies (patch management, AV protection, common configuration)
- Research changes to current desktop management processes to identify the optimum configuration and application changes required for dual stack.
- Virtual Server/Desktop
- Linux
- Windows
- Mac OS
- Test configurations
- Test functionality
- Test security
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy server and desktop services

Task 25 – Network Monitoring for IPv4v6
Activity: Manage all IPv6 assets and ensure alerts when a device drops IPv6, but still operates IPv4. Consider that a coupling with ongoing cybersecurity, interoperability, change management, and patch management activities is necessary as deployment progresses to keep network-monitoring processes up to date.
Objective: Monitor dual stack networks and maintain current monitoring of IPv4 networks.
Specific activities are:

- Define monitoring architecture
- Evaluate dependencies
- Configure monitoring systems
- Configure software to monitor IPv6
- Test dual stack monitoring functionality
- Review any other identified activities required to meet customer needs and approve results for implementation
- Deploy IPv4v6 monitoring

2.5. Disposition

A migration from IPv4 to IPv6 may result in displacement or retirement of equipment. Some equipment does not support IPv6 and is retired, while other equipment is transferred to IPv4 islands or to other organizations. Organizations must plan for the secure disposition of this obsolete equipment, ensuring that no confidential data is released. Organizations place themselves at great risk for exposing confidential information when disposing of obsolete equipment.

Helpful IPv6 links:

ARIN IPv6 Information Center
https://www.arin.net/knowledge/ipv6_info_center.html

NIST Technical Infrastructure for USGv6 Adoption and Testing Program
http://www-x.antd.nist.gov/usgv6/

Digital Government Institute Knowledge Center: IPv6
http://www.digitalgovernment.com/Knowledge-Centers/IPv6.shtml

IPv6 Forum
http://www.ipv6forum.org/

North American IPv6 Task Force
http://www.nav6tf.org/

Rocky Mountain IPv6 Task Force
http://rmv6tf.org/

Federal Communications Commission
http://www.fcc.gov/guides/internet-protocol-version-6-ipv6-consumers

Federal CIO
http://www.cio.gov/Documents/Transition-to-IPv6.pdf

SysAdmin, Audit, Network, Security (SANS) Critical Security Controls
http://www.sans.org/critical-security-controls/

International Information Systems Security Certification Consortium – $(ISC)^2$
https://www.isc2.org/

Internet Engineering Task Force (IETF) Request for Comments (RFC)
https://www.ietf.org/newcomers.html

3. SUMMARY

This document provides an overall process and task approach for dual stack deployment of IPv4v6. Table 4 provides an overview of technical phases and tasks.

Technical Phases	Tasks
Initiation	#1 Develop Baseline IPv6 Knowledge
	#2 Hardware Inventory
	#3 Software Inventory
	#4 Service Inventory
	#5 Operational Support Tools Inventory
	#6 Cybersecurity Tools Inventory
Acquisition/Deployment	#7 Information Service Planning
	#8 IPv6 Numbering Plan
	#9 Develop an IPv6 Test Plan
	#10 Infrastructure and Service Operations Upgrade Plan
	#11 Internal Network Upgrade Plan
	#12 Cost Analysis
Implementation	#13 Build an IPv6 Test Bed
	#14 Cybersecurity
	#15 Update Firewalls for IPv6
	#16 Enable DMZ for IPv6
	#17 Enable External DNS for IPv6
	#18 Enable External WWW for IPv6
	#19 Enable External Email for IPv6
	#20 Enable Other Outbound Services and Applications for IPv6
	#21 Enable Internal Services and Applications for IPv4v6
Operations/Maintenance	#22 Upgrade IP Address Management for IPv4v6
	#23 Enable Active Directory or LDAP and ICAM Services
	#24 Develop Systems Management for IPv4v6
	#25 Network Monitoring for IPv4v6
Disposition	IPv4v6 migration displacement and retirement of equipment

Table 4 Technical Phases and Tasks Overview

The transition from legacy to next generation information and communication technologies is largely uncharted in terms of knowledge, skills, and abilities and information service innovation to come. A literature review of pertinent resources has been conducted to develop a consistent approach to address these challenges and facilitate baked-in security, interoperability, resilient infrastructure, and trusted systems and network design.

The technical phases and tasks are intended for progressive and iterative application, where infrastructure modernization elements are revisited over time to ensure a coordinated and continual level of effort as next generation information and communication technologies evolve. This will keep an organization up to date on its specific goals, objectives, and requirements for information service delivery.

Table 12 provides an overview of infrastructure modernization levels of concern.

Information & Communication Technology Infrastructure Element	Traffic Plane	Information Category	Risk Management	Risk Level	Architecture Level
Services	Command & Control	Classified	Management	High	As-Is
Applications					
Systems	Management	Sensitive	Operational	Medium	Transitional
Networks					
Cybersecurity	User Data	Public	Technical	Low	To-Be
Operational Support					

Table 5 Infrastructure Modernization Levels of Concern Overview

These infrastructure levels of concern form a basis for consistency in this approach to security, interoperability, resilient infrastructure, and trusted systems and network design where cybersecurity and interoperability are primary design requirements. This begins with workforce development to build the requisite knowledge, skills, and abilities necessary for new information and communication technologies and subsequent information service innovation.

Cyberspace modernization is an industry wide challenge with increasing urgency due to the impending North American IPv4 address exhaustion event in early 2015. Additionally, business survivability in the changing global market requires an alignment with economic opportunities to maximize return on investment with new mobile device and mobile network services, and the Internet of Things.

Risk management is exacerbated by the dichotomy of technology and the duplicity of skills required for concurrent legacy and next generation information and communications technology advancement. A full life cycle composition from initiation to disposition comprising a progressive and iterative architectural approach is considered to address these challenges. Also recommended is a combination of likelihood of disruptive event/consequence and difficulty of adversarial attack/consequence analysis to garner probabilistic/quantitative and cyber/qualitative insights to risk management.

4. CONCLUSION

This work identifies a cyberspace modernization approach that touches on many technology areas and considerations. It does not provide in-depth examination of these areas and considerations. Rather, it provides process and task guidance for planning and deployment of IP cyberspace modernization with reference to the "Second Internet" and the "Internet of Things" with the goal of baked-in security, interoperability, resilience, and trust.

Each organization will have distinct management, operational, and technical risks and concerns impacting cyberspace modernization risk management decisions and investment. Decision makers rely on subject matter expertise to make informed decisions. This work has identified subject matter expertise as the most substantial gap standing between legacy and next generation technology deployments, as the differences are significant. Expertise with IPv4 does not imply expertise with IPv6.

Subject matter expertise and depth of technical examination are endeavors that may be satisfied in the phased and iterative approach provided, where knowledge is sought and gained over time (just as it was in the first Internet). The references provided represent several bodies of work that are recommended to those in pursuit of next generation technologies knowledge. The learning curve is a significant challenge when the industry is literally at a pivot point between legacy and next generation technologies.

The "Second Internet" and the "Internet of Things" require a call to action for next generation technical expertise. A significant course of study must be individually and organizationally pursued to successfully attain the requisite skill necessary for secure, resilient, and trusted next generation technology deployments. Organizational investment in training and education starts with executive championship, without which change may be engaged in crisis without the luxury of deterministic planning and development of baked-in security, resilience, and trust. This is necessary to incentivize workforce development.

Cyberspace modernization is evident due to the impending North American IPv4 address exhaustion event. Many consider IPv6 only in the transport protocol and IP address context. Although true, it is not a complete vision and fails to capture the technology suite's breadth and recognition that it is the foundation for new mobile device and mobile network service development and the source of scalability for the Internet of Things.

This document provides process and task guidance with primary consideration given to the secure transition from legacy to next generation technologies. The sweeping, indeed worldwide, rate of change is often omitted in the pursuit of infrastructure preparedness, security, and interoperability. This next generation information assurance and protection approach expands the level of effort to include preparedness, security, interoperability, resilience, and trust in the midst of unprecedented change, vulnerability, threat, and opportunity. We submit that to meet the next generation requirements of interoperability and cybersecurity deterministic planning for security, interoperability, resilience, and trust is necessary. Additionally, such rigor is needed for realization of maximum return on investment.

5. PATH FORWARD

Bridging the digital divide is an ongoing and ever changing proposition, which requires a comprehensive understanding of technological change (Internet + modernization + complexity) and cyber-threat/mitigation practices [26] [27] (risk + cost). The Sandia National Laboratories Tribal Cyber approach to comprehensive security, interoperability, resilience, and trust includes:

- Cyberspace Modernization assessment to understand service, system, network, and security path forward
    - Legacy vs. emergent technologies, for example:
        - RF - Land Mobile Radio (LMR) to APCO Project 25 (P25) digital narrow-banding
        - IPv4 to IPv6
        - Fixed client server to mobility and cloud services
        - Emerging M2M IP communications
- Quantitative risk (probabilistic) assessment to increase protection against predictable events
- Qualitative risk (difficulty) assessment to increase protection against human element events
- Adversary-Based Security assessment to increase protection against adversarial cyber attack
- Resilient Infrastructure Systems analysis to ensure resilience to disruptive events
- Trusted and Secure Systems analysis to ensure fail-secure operations during service degradation
- Continuity/Human element/Cyber training and exercises to increase knowledge and awareness and inform decision makers, operators, and security practitioners
- Energy efficient Data Center design and virtualized infrastructure
- Cyberspace Modernization research and development including modeling, simulation, and emulation of complex systems

This set of specific capabilities for comprehensive assessment and analysis of cyberspace systems and infrastructure modernization are applicable across all critical infrastructure sectors while retaining the agility for application to specific sector systems, such as FirstNet [31].

Challenge equals opportunity. There is a worldwide shift from circuit switched technologies to packet switched technologies that precipitates not only a migration to predominant IP communications, but also concurrently IPv4 to IPv6. It is anticipated that at such time as IPv6 becomes predominant, economic factors, such as the cost to develop, deliver, and maintain next generation information services, will motivate a global shift to all IPv6. Whether that is five, ten, or twenty years is up for debate. The oft used axiom “knowledge is power” applies to technological innovation. IPv6 subject matter expertise could become a common capability within a five-year timeframe due to IPv4 exhaustion and the continual growth in mobility, mobile networks, and M2M interconnectivity. The question is “How secure, resilient, and trusted will your information assets be? Our intent is to provide a path to informed decisions to answer that question.

Work to adapt to a shifting cyberspace and its associated threats is ongoing. A May 2014 NIST special publication 800-160 initial public draft: System Security Engineering, An Integrated Approach to Building Trustworthy Resilient Systems [32] provides a formal system engineering approach to address security issues from a stakeholder requirements and needs perspective. Additionally, a DHS Cyber Resilience Review [33] includes a February 2014 mapping to the NIST Cybersecurity Framework.

In closing, this document addresses next generation information assurance and is written for decision makers of organizations dependent on information and communication technologies innovation and therefore, IPv6. This document also addresses implementation and is written to inform the operators, practitioners, engineers, and architects with responsibility for the maintenance, operations, security, and modernization of information systems and networks.

This document merely touches many areas of technology and does not address exhaustive methods to organizational investment decisions. The guidance provided herein is intended for the secure deployment of IPv6, which will mature as the proliferation of next generation technologies continues and the requisite level of expertise reaches across the communications, IT, and other sectors. The sooner an organization invests in training and education the sooner that organization will be able to deterministically manage next generation technologies challenges, risks and opportunities and realize a maximum return on investment.

The intention is to advocate organizational and individual pursuit of expertise to fill the gap of knowledge and to encourage development of the skills necessary for secure deployment of next generation advanced information services. Seasoned ICT professionals face a significant learning curve in regard to next generation advanced information services, and many people are over tasked as organizations mitigate competing priorities and financial constraints. This makes the pursuit of next generation expertise difficult in terms of time and motivation, where only the most ambitious may take on the added workload to get ahead. To the organization, our advice is to establish executive championship to facilitate workforce development. To the individual, our advice is to prepare for the rest of your career and enjoy the endeavor.

REFERENCES

1. Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC): 2460, “Internet Protocol, Version 6 (IPv6) Specification” December 1998. http://www.rfc-editor.org/rfc/rfc2460.txt
2. IETF Network Working Group RFC: 1881 "IPv6 Address Allocation Management", December 1995. http://www.rfc-editor.org/rfc/rfc1881.txt
3. IETF Network Working Group RFC: 2401 "Security Architecture for the Internet Protocol", November 1998. http://www.rfc-editor.org/rfc/rfc2401.txt
4. NIST SP 800-119: Guidelines for the Secure Deployment of IPv6, http://csrc.nist.gov/publications/PubsSPs.html
5. Cisco Press: Deploying IPv6 Networks: ISBN-13-1-58705-210-5, http://www.ciscopress.com/store/deploying-ipv6-networks-9781587052101
6. Cisco Press: IPv6 Security: ISBN-13 978-1-58705594, http://www.hoggnet.com/ , http://www.ciscopress.com/store/ipv6-security-9781587055942
7. Department of Homeland Security (DHS) National Infrastructure Protection Plan 2013. https://www.dhs.gov/national-infrastructure-protection-plan
8. IETF Network Working Group RFC 4861 “Neighbor Discovery for IP version 6 (IPv6)”, September 2007, http://www.rfc-editor.org/rfc/rfc4861.txt
9. IETF Network Working Group RFC "IPv6 Stateless Address Autoconfiguration", September 2007, http://www.rfc-editor.org/rfc/rfc4862.txt
10. Office of Management and Budget IPv6 Federal Mandates: transition-to-ipv6-1.pdf http://www.whitehouse.gov/omb/memoranda_default
11. IETF Network Working Group RFC: 3775 "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", June 2004. http://www.rfc-editor.org/rfc/rfc3776.txt
12. IETF Network Working Group RFC: 4877 “Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture”, April 2007. http://www.rfc-editor.org/rfc/rfc4877.txt
13. IETF Network Working Group RFC: 6275 "Mobility Support in IPv6", July 2011. http://www.rfc-editor.org/rfc/rfc6275.txt
14. IETF Network Working Group RFC: 6618 "Mobile IPv6 Security Framework Using Transport Layer Security for Communication between the Mobile Node and Home Agent", May 2012. http://www.rfc-editor.org/rfc/rfc6618.txt
15. IETF Network Working Group RFC: 6459 "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", January 2012. http://www.ietf.org/rfc/rfc6459.txt
16. Microsoft, Inc.: Networking and Access Technologies – TCP/IP v4 and v6: “Windows Server 2008 and Windows Vista TCP/IP was completely redesigned to support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).” http://technet.microsoft.com/en-us/network/bb530961.aspx
17. Microsoft, Inc.: Lync Server - Planning for and Configuring IPv6: “Lync Server 2013 includes support for IP version 6 (IPv6) addresses.” http://technet.microsoft.com/en-us/library/jj204624.aspx
18. Red Hat, Inc.: Red Hat Enterprise Linux Is Ready: “with complete IPv6 implementations shipping today in Red Hat Enterprise Linux version 5 and 6 and Fedora.” http://www.redhat.com/about/news/archive/2011/6/rhelipv6blog

19. Cisco Systems, Inc.: IPv6: “As the Internet transitions, organizations must adopt IPv6 to support future business continuity, growth, and global expansion.” http://www.cisco.com/web/solutions/trends/ipv6/index.html
20. Juniper Networks, Inc.: IPv6: “Juniper Networks has made significant investments in technologies and solutions that enable enterprises and service providers to meet mixed IP addressing needs even as they build out IPv6 networks as rapidly as markets and services require.” http://www.juniper.net/us/en/company/innovation/ipv6/
21. Brocade Communication Systems, Inc.: IPv4 Addresses Dry Up; Brocade Customers Years Ahead With Proven IPv6-Ready Solutions: http://newsroom.brocade.com/press-releases/ipv4-addresses-dry-up-brocade-customers-years-ahe-nasdaq-brcd-0765358
22. IETF Informational RFC: 7123 "Security Implications of IPv6 on IPv4 Networks", February 2014. http://www.rfc-editor.org/rfc/rfc7123.txt
23. National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL): http://www.nist.gov/itl/antd/usgv6.cfm
24. National Telecommunications and Information Administration (NTIA) Technical and Economic Assessment of Internet Protocol Version 6 (IPv6): http://www.ntia.doc.gov/report/2006/technical-and-economic-assessment-internet-protocol-version-6-ipv6
25. NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations: http://csrc.nist.gov/publications/PubsSPs.html
26. SysAdmin, Audit, Network, Security Institute (SANS) 20 critical security controls (CSC), http://www.sans.org/critical-security-controls/
27. SysAdmin, Audit, Network, Security Institute (SANS) 20 critical security controls (CSC): Appendix A: Mapping between the Critical Controls and National Institute of Standards and Technology Special Publication 800-53, Revision 3, Priority 1 Items, http://www.sans.org/critical-security-controls/guidelines.php
28. SAND2013-38616 Analysis of Alternatives for Risk Assessment Methodologies and Tools, October 2013, Noel M. Nachitigal, Julia A. Fruetel, Nathaniel J. Gleason, Jovana Helms, Dennis R. Imbro, and Matthew C. Sumner: Available to the public from the U.S Department of Commerce National Technical Information Service, 5285 Port Royal Rd. Springfield, VA 22161, (800)553-6847, Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online
29. Executive Order 13636: Improving Critical Infrastructure Cybersecurity, February 12, 2013: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
30. NIST Cybersecurity Framework Version 1.0, February 12, 2014: http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm
31. Department of Homeland Security and Department of Commerce FirstNet initiative: http://www.firstnet.gov/
32. NIST SP 800-160: System Security Engineering, An Integrated Approach to Building Trustworthy Resilient Systems. Initial Public Draft May 2014, http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf
33. DHS Cyber Resilience Review: www.us-cert.gov/ccubedvp/self-service-crr

APPENDIX A: IPV6 NEXT GENERATION INFORMATION ASSURANCE AND PROTECTION

IPv6 Protocol Protection

Next generation information assurance and protection assessment includes IPv6 protocol protections for secure deployment[4]. Further research is needed to mitigate legacy and next generation IP threats, vulnerabilities, and risk exposure as deployment progresses.

IPv6 Protocol Threats/Vulnerabilities	Mitigations
Internet Control Message Protocol (ICMPv6) Messages	Hop Limit set to 255 for Router Solicitation (RS) Type 133, Router Advertisement (RA) Type 134, Neighbor Solicitation (NS) Type 135, Neighbor Advertisement (NA) Type 136, Redirection Type 137, Inverse Neighbor Discovery (ND) Solicitation Type 141 and Advertisement Type 142, Certificate Path Solicitation (Secure Neighbor Discovery (SEND) Type 148 and Advertisement Type 149
ICMPv6 unallocated and experimental Messages	Deny ICMPv6 echo response from outside, allow Destination Unreachable Type 1, Packet Too Big Type 2, Time Exceeded Type 3, Parameter Problem Type 4
Extension Header Threats	Network perimeter filtering, IDS/ Network IDS (NIDS)
Extension Header Vulnerabilities	Network perimeter filtering, Intrusion Detection, Deep Packet Inspection (DPI)
Routing Header 0	Network perimeter filtering to explicitly deny all RH0 option headers, Intrusion Detection, DPI
IPv6 Extension Header Fuzzing	Network perimeter filtering to explicitly permit essential ICMPv6 traffic and specific use DNS [53], web [80,443], and email [25] services. Deny all others. Intrusion Detection and DPI
Router Alert Attack	Network perimeter filtering, IDS
Rogue Router Advertisement (RA)	RA Guard
Fragmentation Header	Virtual Fragment Reassembly (VRF) (Cisco), Intrusion Detection, DPI
Unknown Option Headers	Intrusion Detection, DPI
Upper Layer Headers	Intrusion Detection, DPI, Proxy and Application Layer Gateway (ALG) packet disassembly and reassembly
Reconnaissance/Scanning and Assessing	Network perimeter filtering, IDS
Registry Checking	Network perimeter filtering, IDS
Multicast Reconnaissance Layer 3 and 4 Spoofing	Network perimeter filtering, IDS

Table A-1 IPv6 Protocol Threats Vulnerabilities and Mitigations

[4] Information sources include the Internet Engineering Task Force (IETF) Requests for Comment (RFC), Cisco Press: IPv6 Security: ISBN-13 978-1-58705594, Deploying IPv6 Networks: ISBN-13-1-58705-210-5, NIST SP 800-53, and the SysAdmin, Audit, Network, Security Institute (SANS) 20 critical security controls (CSC).

IPv6 and Internet Threats	Mitigations
Packet Flooding	Network Perimeter Filtering, Rate Limiting
Internet Worms	Network Perimeter Filtering, IDS, Virus Protection
Distributed Denial of Service (DDOS)	Network Perimeter Filtering, IDS, Rate Limiting
Man in the Middle	Encryption, Generic Routing Encapsulation (GRE), IPSec VPN
Botnets	Network Perimeter Filtering, IDS, Data Loss Prevention (DLP)
Bogon Addresses	Network Perimeter Filtering
BGP Time-to-Live (TTL), Long autonomous system (AS) paths, Private AS paths	Network Perimeter Filtering, BGP Authentication, Hop Limit set to 255 - Generalized TTL-based Security Mechanism (GTSM)
IGP Prefix Delegation Threats	Network Perimeter Filtering, IDS
SLAAC Predictability	Dynamic Host Configuration Protocol (DHCPv6), Cryptographically Generated Addresses (CGA), Randomly Generated Addresses, Manually Configured Addresses
Multi-homing Issues	Provider Independent (PI) IPv6 address Allocation as opposed to Provider Aggregatable (PA) IPv6 address Allocation, Site Multihoming by IPv6 Intermediation (SHIM6)

Table A-2 IPv6 Internet Threats and Mitigations

Routes to Block Inbound and Outbound at the Network Perimeter	Prefixes
Default route	::/0
Unspecified address	::/128
Loopback address	::1/128
IPv4-compatible address	::/96
IPv4-mapped address	::ffff:0.0.0.0/96
Link-local addresses	fe80::/10 or longer
Site-local addresses (depreciated)	fec0::/10 or longer
Unique-local addresses	fc00::/7 or longer
Multicast addresses	ff00::/8 or longer
Documentation addresses	2001:db8::/32 or longer
6Bone addresses	3ffe::/16

Table A-3 IPv6 Routes to Block Inbound and Outbound

IPv6 Network Technical Risks	Mitigations
Automatic IPv6 Tunneling – 6to4, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), Teredo may erode perimeter protection if permitted to tunnel unabated	Automated tunneling should be carefully considered and used only when required. Generally, the filtering of protocol 41 protests against automated tunneling, additional parameters include Ethernet frame protocol type field 0x86dd, protocol version set to 6, an IPv6 destination address 2001::/32, IPv4 address 192.88.99.0/24 (well known tunnel relay address), User Datagram Protocol (UDP) port 3544 for Teredo, IPv4 address 239.0.0.0/8 (well known multicast address), Transmission Control Protocol (TCP) and UDP port 3653 for Tunnel Setup Protocol (TSP), UDP/TCP port 5072 for Anything in Anything (AYIYA)
Man in the Middle	Encryption, Generic Routing Encapsulation (GRE), IPSec VPN
Botnets	Network Perimeter Filtering, IDS, Data Loss Prevention (DLP)
Bogon Addresses	Network Perimeter Filtering
BGP Time-to-Live (TTL), Long autonomous system (AS) paths, Private AS paths	Network Perimeter Filtering, BGP Authentication, Hop Limit set to 255 - Generalized TTL-based Security Mechanism (GTSM)
IGP Prefix Delegation Threats	Network Perimeter Filtering, IDS
SLAAC Predictability	Dynamic Host Configuration Protocol (DHCPv6), Cryptographically Generated Addresses (CGA), Randomly Generated Addresses, Manually Configured Addresses
Multi-homing Issues	Provider Independent (PI) IPv6 address Allocation as opposed to Provider Aggregatable (PA) IPv6 address Allocation, Site Multihoming by IPv6 Intermediation (SHIM6)

Table A-4 IPv6 Network Technical Risks

New Threat Considerations and Mitigations

IPv6 New Threat Considerations	IPv6 Characteristics	Mitigations
Reconnaissance	Scanning for hosts is not feasible due to large address space. Well-known addresses, in particular multicast, are vulnerable. Dual stack overlay may reduce the field of hosts necessary to scan for reconnaissance due to correlated IPv4/v6 addresses.	Same as IPv4. Privacy extensions make reconnaissance less effective.
Unauthorized access	End-to-end security reduces the exposure, Extension headers (EH) open new attack venues.	Use Privacy extensions to reduce host exposure. Use multiple addresses with different scopes. Manage EH use.
Header manipulation	IPv6 can take advantage of chained and large EH's. EH's that must be processed by all stacks are particularly useful to an attacker.	EH usage should be strictly controlled based on deployed services. Block RH 0 EH's.
Fragmentation	No fragment overlap should be allowed in IPv6, but some stacks do reassemble overlapping fragments. The impact of tiny fragments is minimal in IPv6.	Use properly implemented stacks that do not process overlapping fragments. Note that only source and destination hosts not routers process fragmented packets.
Layer3/layer 4 spoofing	The use of tunneling offers more spoofing opportunities even though they are not different from IPv4 tunneling.	Same mitigation techniques as IPv4.
Host initialization and address resolution attacks	DHCP has similar vulnerabilities for IPv4 and IPv6.Neighbor discovery has similar vulnerabilities as ARP. Stateless Auto-configuration and renumbering offer new attack options.	Use an interim solution such as static neighbors; SEND recommendations adopted by the IPv6 stacks.
Broadcast amplification attacks (Smurf)	No concept of broadcast in IPv6, and that reduces amplification options.	Use filtering for multicast traffic because it is the only amplification option.

New Threat Considerations and Mitigations (Cont)

IPv6 New Threat Considerations	IPv6 Characteristics	Mitigations
Routing attacks	IPSec provides additional peering security for some routing protocols. From a threat perspective it is similar to IPv4.	Same as IPv4. Implement IPSec whenever possible.
Viruses and worms	Same as IPv4. Random scanning used by worms to propagate is impractical in IPv6 because of the large address space.	Same as IPv4. In particular host based virus protection.
Transition mechanism attacks	New ports to open in IPv4 firewalls. Automatic tunnels are more susceptible to attacks. IPv6-IPv4 translation can hide the source of attacks.	Tighter control of ports opened in firewalls; open only necessary ports. Use static tunnels when possible.
Mobile IP/NEMO	Embedded in IPv6, has specific security features (IPSec, IKE, TLS).	Filter out all routing headers except type 2 if MIPv6 is used. Securing MIPv6 beyond IPSec is a work in process.

Table A-5 IPv6 New Threat Considerations and Mitigations

IPv6 and IPv4 Similar Threats and Mitigations

IPv6 and IPv4 Similar Threats	IPv6 Characteristics	Mitigations
Sniffing	Same as IPv4.	Same as IPv4.
Application layer attacks	IPSec offers the potential to increase security and to track attackers.	Similar to IPv4, security ultimately relies on host defenses.
Rogue devices	Same as IPv4, although mobility is increasing and hence increasing the threat (Bring Your Own Device) which can also act as mobile access points	IPSec can prevent interaction with such devices. Lower-layer protocols such as 802.1x can be used to block unauthorized devices from connecting to the network.
Man-in-the-middle attacks	IPSec can protect so long as the key is not stolen.	There is a need for a scalable and operationally feasible authentication and key-exchange mechanism.
Flooding attacks	Same as IPv4, with a few additional traffic types.	Use traffic-limiting options.

Table A-6 IPv6 and IPv4 Similar Threats and Mitigations

APPENDIX B: SANS 20 CSC TO NIST 800-53

Critical Security Controls (CSC) v4.1 to NIST 800-53 rev4 – Executive Summary

ID	BS ISO/IEC 27001:2005 Annex A - Control Objectives and Controls	Gap Analysis	Matching Controls
CSC #1	Inventory of Authorized and Unauthorized Devices	SC included in NIST 800-53	CA-7: Continuous Monitoring CM-8: Information System Component Inventory IA-3: Device Identification and Authentication SA-4: Acquisition Process SC-17: Public Key Infrastructure Certificates SI-4: Information System Monitoring PM-5: Information System Inventory
CSC #2	Inventory of Authorized and Unauthorized Software	SC included in NIST 800-53	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-8: Information System Component Inventory CM-10: Software Usage Restrictions CM Acquisition Process SC-18: Mobile Code SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring PM-5: Information System Inventory
CSC #3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	SC included in NIST 800-53	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation
CSC #4	Continuous Vulnerability Assessment and Remediation	SC included in NIST 800-53	CA-2: Security Assessments CA-7: Continuous Monitoring RA-5: Vulnerability Scanning SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring SI-7: Software, Firmware, and Information Integrity
CSC #5	Malware Defenses	SC included in NIST 800-53	CA-7: Continuous Monitoring SC-39: Process Isolation SC-44: Detonation Chambers SI-3: Malicious Code Protection SI-4: Information System Monitoring SI-8: Spam Protection
CSC #6	Application Software Security	SC included in NIST 800-53	SA-13: Trustworthiness SA-15: Development Process, Standards, and Tools SA-16: Developer-Provided Training SA-17: Developer Security Architecture and Design SA-20: Customized Development of Critical Components SA-21: Developer Screening SC-39: Process Isolation SI-10: Information Input Validation SI-11: Error Handling SI-15: Information Output Filtering SI-16: Memory Protection

Mapping the CSC v4.1 to NIST 800-53 rev4 – Executive Summary (Cont)

CSC #7	Wireless Device Control	SC included in NIST 800-53	CSC 9.1-9.6 AC-18: Wireless Access AC-19: Access Control for Mobile Devices CA-3: System Interconnections CA-7: Continuous Monitoring CM-2: Baseline Configuration IA-3: Device Identification and Authentication SC-8: Transmission Confidentiality and Integrity SC-17: Public Key Infrastructure Certificates SC-40: Wireless Link Protection SI-4: Information System Monitoring
CSC #8	Data Recovery Capability	SC included in NIST 800-53	CP-9: Information System Backup CP-10: Information System Recovery and Reconstitution MP-4: Media Storage
CSC #9	Security Skills Assessment and Appropriate Training to Fill Gaps	SC included in NIST 800-53	AT-1: Security Awareness and Training Policy and Procedures AT-2: Security Awareness Training AT-3: Role-Based Security Training AT-4: Security Training Records SA-11: Developer Security Testing and Evaluation SA-16: Developer-Provided Training PM-13: Information Security Workforce PM-14: Testing, Training, & Monitoring PM-16: Threat Awareness Program
CSC #10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	SC included in NIST 800-53	AC-4: Information Flow Enforcement CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-8: Information System Component Inventory MA-4: Nonlocal Maintenance SC-24: Fail in Known State SI 4: Information System Monitoring
SC #11	Limitation and Control of Network Ports, Protocols, and Services	SC included in NIST 800-53	AC-4: Information Flow Enforcement CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-6: Configuration Settings CM-8: Information System Component Inventory SC-20: Secure Name /Address Resolution Service (Authoritative Source) SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver) SC-22: Architecture and Provisioning for Name/Address Resolution Service SC-41: Port and I/O Device Access
CSC #12	Controlled Use of Administrative Privileges	SC included in NIST 800-53	AC-2: Account Management AC-6: Least Privilege AC-17: Remote Access AC-19: Access Control for Mobile Devices CA-7: Continuous Monitoring IA-2: Identification and Authentication (Organizational Users) IA-4: Identifier Management IA-5: Authenticator Management SI-4: Information System Monitoring

Mapping the CSC v4.1 to NIST 800-53 rev4 – Executive Summary (Cont)

CSC #13	Boundary Defense	SC included in NIST 800-53	AC-4: Information Flow Enforcement AC-17: Remote Access AC-20: Use of External Information Systems CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration SA-9: External Information System Services SC-7: Boundary Protection SC-8: Transmission Confidentiality and Integrity SI-4: Information System Monitoring
CSC #14	Maintenance, Monitoring, and Analysis of Audit Logs	SC included in NIST 800-53	AC-23: Data Mining Protection AU-2: Audit Events AU-3: Content of Audit Records AU-4: Audit Storage Capacity AU-5: Response to Audit Processing Failures AU-6: Audit Review, Analysis, and Reporting AU-7: Audit Reduction and Report Generation AU-8: Time Stamps AU-9: Protection of Audit Information AU-10: Non-repudiation AU-11: Audit Record Retention AU-12: Audit Generation AU-13: Monitoring for Information Disclosure AU-14: Session Audit CA-7: Continuous Monitoring IA-10: Adaptive Identification and Authentication
CSC #15	Controlled Access Based on the Need to Know	SC included in NIST 800-53	AC-1: Access Control Policy and Procedures AC-2: Account Management AC-3: Access Enforcement AC-6: Least Privilege AC-24: Access Control Decisions CA-7: Continuous Monitoring MP-3: Media Marking RA-2: Security Categorization SC-16: Transmission of Security Attributes SI-4: Information System Monitoring
CSC #16	Account Monitoring and Control	SC included in NIST 800-53	AC-2: Account Management AC-3: Access Enforcement AC-7: Unsuccessful Logon Attempts AC-11: Session Lock AC-12: Session Termination CA-7: Continuous Monitoring IA-5: Authenticator Management IA-10: Adaptive Identification and Authentication SC-17: Public Key Infrastructure Certificates SC-23: Session Authenticity SI-4: Information System Monitoring

Mapping the CSC v4.1 to NIST 800-53 rev4 – Executive Summary (Cont)

CSC #17	Data Loss Prevention	SC included in NIST 800-53	AC-3: Access Enforcement AC-4: Information Flow Enforcement AC-23: Data Mining Protection CA-7: Continuous Monitoring CA-9: Internal System Connections IR-9: Information Spillage Response MP-5: Media Transport SA-18: Tamper Resistance and Detection SC-8: Transmission Confidentiality and Integrity SC-28: Protection of Information at Rest SC-31: Covert Channel Analysis SC-41: Port and I/O Device Access SI-4: Information System Monitoring
CSC #18	Incident Response and Management	SC included in NIST 800-53	IR-1: Incident Response Policy and Procedures IR-2: Incident Response Training IR-3: Incident Response Testing IR-4: Incident Handling IR-5: Incident Monitoring IR-6: Incident Reporting IR-7: Incident Response Assistance IR-8: Incident Response Plan IR-10: Integrated Information Security Analysis Team
CSC #19	Secure Network Engineering	SC included in NIST 800-53	AC-4: Information Flow Enforcement CA-3: System Interconnections CA-9: Internal System Connections SA-8: Security Engineering Principles SC-20: Secure Name /Address Resolution Service (Authoritative Source) SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver) SC-22: Architecture and Provisioning for Name/Address Resolution Service SC-32: Information System Partitioning SC 37: Out of Band Channels
CSC #20	Penetration Tests and Red Team Exercises	SC included in NIST 800-53	CA-2: Security Assessments CA-5: Plan of Action and Milestones CA-6: Security Authorization CA-8: Penetration Testing RA-6: Technical Surveillance Countermeasures Survey SI-6: Security Function Verification PM-6: Information Security Measures of Performance PM-14: Testing Training & Monitoring

Table B-1 Mapping the Critical Security Controls to NIST 800-53

APPENDIX C: TECHNICAL ACRONYMS

6rd – IPv6 Rapid Deployment
AAA - Authentication, Authorization, and Accounting
ACL – Access Control List
ALG - Application Layer Gateway
ARP – Address Resolution Protocol
AS – Autonomous System
ATM – Asynchronous Transfer Mode
AV – Anti-Virus
AYIYA - Anything in Anything
BIND - Berkeley Internet Name Domain
BGP - Border Gateway Protocol
CGA - Cryptographically Generated Addresses
CN - Correspondent Node
CPE – Customer Premise Equipment
CSC – SANS Critical Security Controls
Cyber CIP - Cyber Critical Infrastructure Protection
DaaS – Desktop as a Service
DDOS - Distributed Denial of Service
DHCP - Dynamic Host Configuration Protocol
DiffServ - Differentiated Services
DLP - Data Loss Prevention
DMZ – Demilitarized or Demarcation Zone Network
DNS - Domain Name System
DNSSEC - DNS Security Extensions
DPI - Deep Packet Inspection
DUID - DHCP unique identifiers
EH - Extension headers
ES&H – Environmental Safety & Health
ESP - Encapsulating Security Payload
EUI-64 - Extended Unique Identifier on 64 bits address
E-UTRAN - Evolved-Universal Terrestrial Radio Access Network
GPS - Global Positioning Systems
GRE - Generic Routing Encapsulation
GTSM - Generalized TTL-based Security Mechanism
HA - Home Agent
HAC - Home Agent Controller
HIDS – Host Intrusion Detection System
HTTP - Hypertext Transfer Protocol
IaaS - Infrastructure as a Service
ICAM – Identity Credential and Access Management
ICMP – Internet Control Message Protocol
IDS - Intrusion Detection System
IGP – Interior Gateway Protocols
IKE - Internet Key Exchange
IMAP - Internet Message Application Protocol
IPAM – IP Address Management
IPS - Intrusion Prevention System
IPsec - Internet Protocol Security
IPv4v6 - IPv4 and IPv6 (dual stack)
IR – Incident Response
ISAC - Information Sharing & Analysis Centers
ISATAP - Intra-Site Automatic Tunneling Addressing Protocol
ISP – Internet Service Provider
ITDR - Information Technology Disaster Recovery
LDAP – Lightweight Directory Access Protocol
LTE – Long Term Evolution
MAC – Media Access Control address
MIBs - Management Information Base
MIP - Mobile IP
MLDV - Multicast Listener Discovery version
MN - Mobile Node
MPLS - Multiprotocol Label Switching
MTA - Mail Transfer Agent
NAT - Network Address Translation
NDP - Neighbor Discovery Protocol
NEMO - Network Mobility
NA - Neighbor Advertisement
ND – Neighbor Discovery
NIDS – Network Intrusion Detection System
NS - Neighbor Solicitation

NTP – Network Time Protocol
OSPF – Open Shortest Path First
OSS - Operational Support Systems
P25 – APCO Project 25
PA - Provider Aggregatable Address
PaaS - Platform as a Service
PI - Provider Independent address
PIM-SM - Protocol Independent Multicast-Spare Mode
PKI - Public Key Infrastructure
PRA - Probabilistic Risk Assessment
PSAP - Public Safety Answering Point
PSTN – Public Switched Telephone Network
PTP - Point-to-Point
QoS - Quality of Service
QRA – Qualitative Risk Assessment
RA - Risk Assessment and Router Advertisement
RDNC – Remote Name Daemon Control
RFID - Radio Frequency Identification
RH – Routing Header
RIMES – Risk-Informed Management of Enterprise Security
RIR – Regional Internet Registry
ROHC - Robust Header Compression
RS - Router Solicitation
SaaS - Software as a Service
SEND – Secure Neighbor Discovery
SC - System and Communications Protection
SCADA - Supervisory, Control and Data Acquisition
SHIM6 - Site Multihoming by IPv6 Intermediation
SIIT - Stateless IP/ICMP Translation Algorithm
SIP – Session Initiation Protocol
SLA - Service Level Agreement
SLAAC - Stateless Address Automated Configuration
SNMP - Simple Network Management Protocol
SMTP – Simple Mail Transfer Protocol
SSL – Secure Sockets Layer
TCP – Transmission Control Protocol
TLD – Top Level Domain
TLS – Transport Layer Security
TSP - Tunnel Setup Protocol
TTL – Time to Live
UDP - User Datagram Protocol
ULA - Unique Local Address
URI – Uniform Resource Identifier
VDT – Virtual Desktop
VoIP - Voice over Internet Protocol
VRF - Virtual Fragment Reassembly
VPN - Virtual Private Network

DISTRIBUTION

1	MS0174	Lita Suina	042365 (electronic copy)
1	MS0503	Benjamin Mar	05337 (electronic copy)
1	MS0513	Kevin Robbins	05337 (electronic copy)
1	MS0529	David A. Wiegandt	05337 (electronic copy)
1	MS0671	Alexander W. Roesler	05627 (electronic copy)
1	MS0671	Raymond C. Parks	05627 (electronic copy)
1	MS0671	William D. Atkins	06612 (electronic copy)
1	MS0671	Benjamin R. Anderson	06612 (electronic copy)
1	MS0671	John Bailon	05623 (electronic copy)
1	MS0748	F. Mitch McCrory	06231 (electronic copy)
1	MS0757	Shawn E. Taylor	06612 (electronic copy)
1	MS0769	Robert L. Hutchinson	08970 (electronic copy)
1	MS0801	John D. Zepper	09300 (electronic copy)
1	MS0806	Jeremy L. Banks	09336 (electronic copy)
1	MS0813	Beth A. Potts	09312 (electronic copy)
1	MS0820	Robert A. Mason	09338 (electronic copy)
1	MS0820	John P. Abbott	09338 (electronic copy)
1	MS0823	Patrick L. Manke	09335 (electronic copy)
1	MS0823	Anthony D. Perea	09324 (electronic copy)
1	MS0832	Kenneth A. Bernier	09335 (electronic copy)
1	MS0838	G. Kelly Rogers	09330 (electronic copy)
3	MS0838	Victor N. McLane	09324
1	MS1027	Cheston E. Bailon	05635 (electronic copy)
1	MS1113	Kenneth Martinez-Eubanks	042375 (electronic copy)
1	MS1137	Andjelka Kelic	06924 (electronic copy)
1	MS1137	Barbara J. Jennings	06924 (electronic copy)
1	MS1138	Lori K. Parrott	06924 (electronic copy)
3	MS1324	Curtis M. Keliiaa	09336
1	MS1326	LeAnn A. Miller	01460 (electronic copy)
1	MS1327	Kevin S. Nauer	09312 (electronic copy)
1	MS1371	Ronald H. Mori	06832 (electronic copy)
1	MS1466	Laurence E. Brown	00166 (electronic copy)
1	MS9004	Heidi R. Ammerlahn	08960 (electronic copy)
1	MS9012	Tracy R. Walker	08949 (electronic copy)
1	MS9012	Rich Gay	08949 (electronic copy)
1	MS9407	Nathaniel J. Gleason	08116 (electronic copy)
1	MS0932	Tim L. MacAlpine	09517 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories