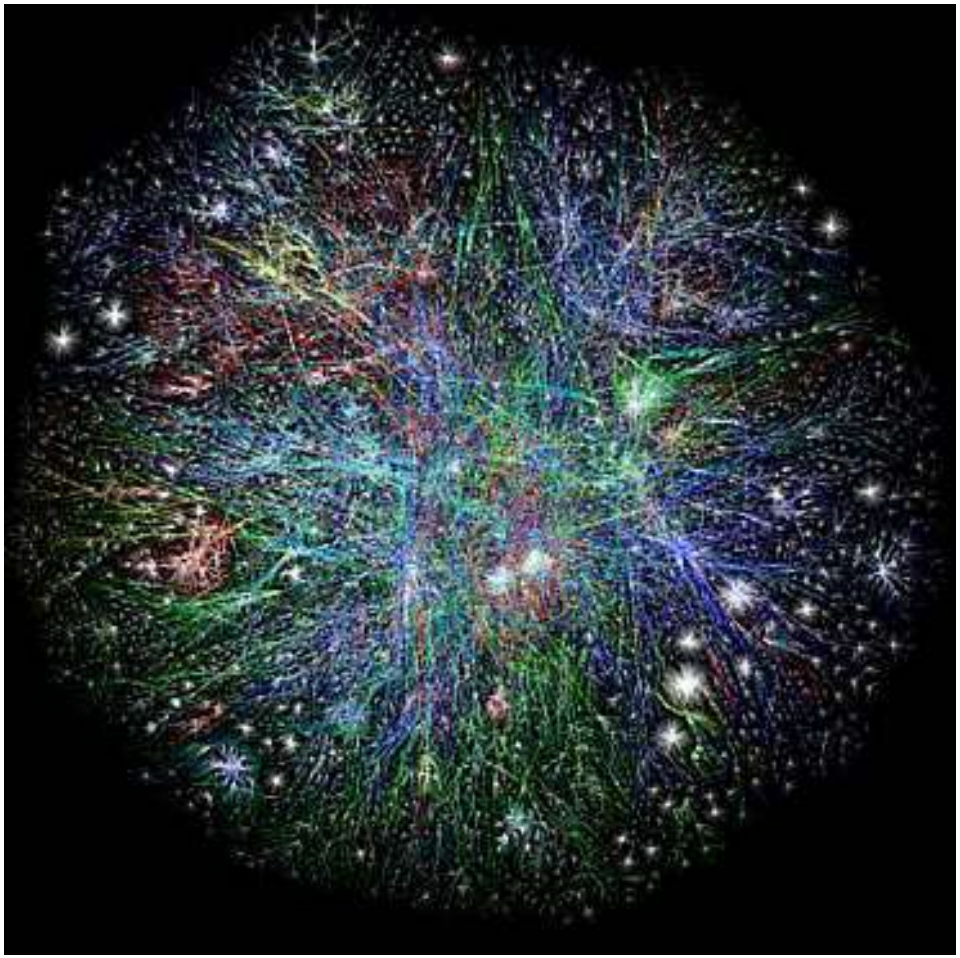
Use of the Federal IPv6 **Roadmap** for Enterprise Transition Guidance and Planning

John L. Lee, Internet Associates, LLC

Rocky Mountain IPv6 Task Force

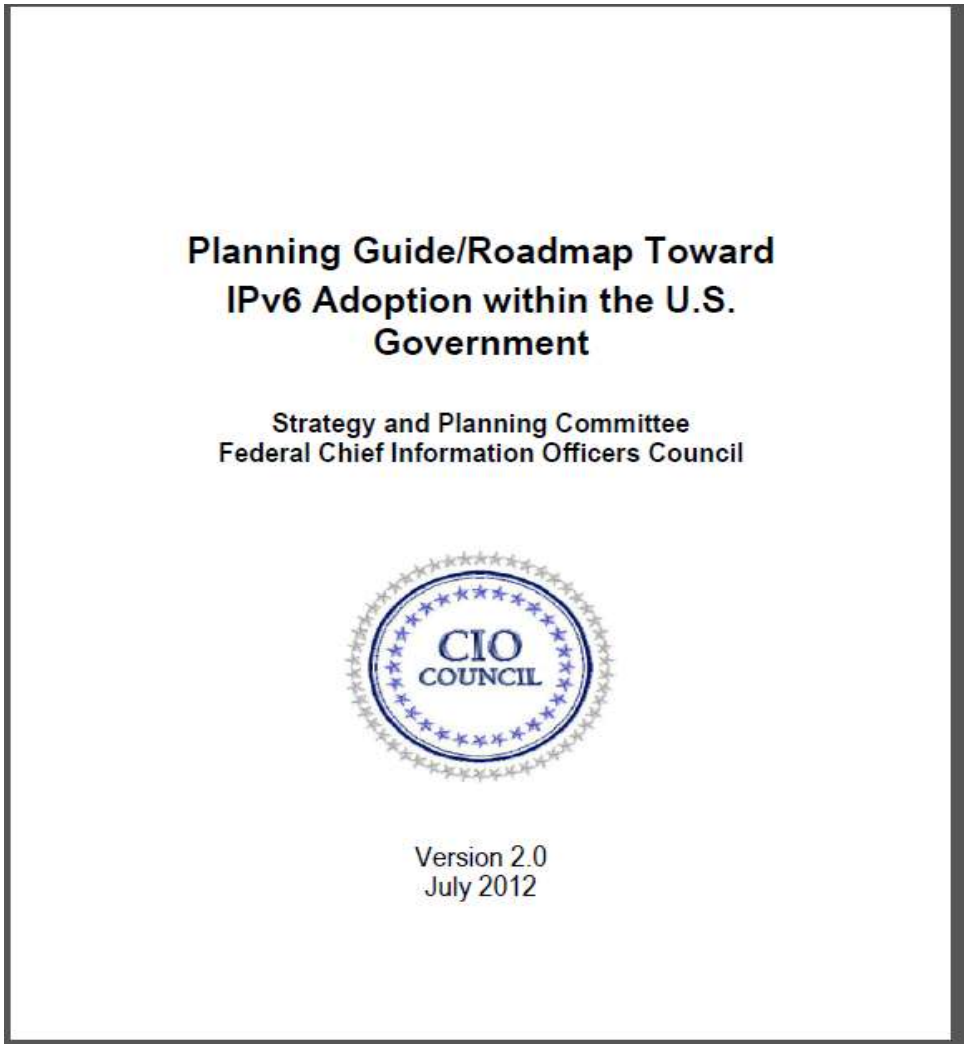
RMv6TF

When you have a number of paths?



You Need a Map

Better yet a Guide or Roadmap



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

Strategy and Planning Committee
Federal Chief Information Officers Council

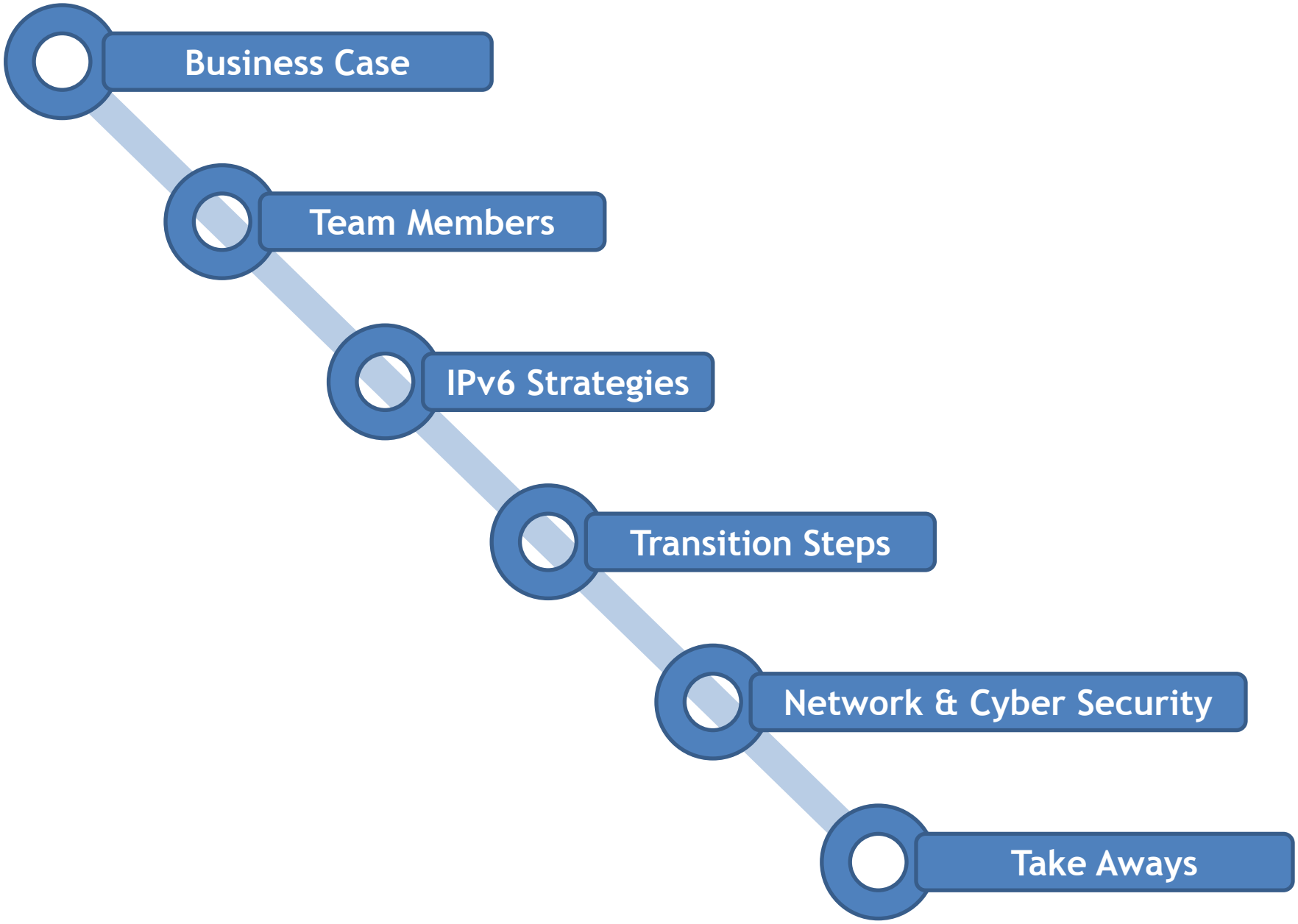
CIO COUNCIL

Version 2.0
July 2012

Before we start our journey

As your Guide …

The opinions contained in this brief are those of the author and do not reflect an opinion or official position of the United States Government, ACT-IAC, Internet Associates or any other entity


Business Case
Team Members
IPv6 Strategies
Transition Steps
Network & Cyber Security
Take Aways


Business Case

Business (Governance) Objectives

- Ubiquitous citizen services to larger number of citizens at lower costs
  - More targeted and focused services
- High speed Broadband Access
- Enhanced education and healthcare delivery
- Increased Rural economic activity

Delivery of Ubiquitous Services Equal Access

Cloud First Strategy

Enterprise Business Case

1. International customers with v6 only phones can only reach your competitors web site
2. Hackers gain a pivot system and use v6 tunneling to hack other countries systems (FBI pays you a visit)
3. Investors sense you are behind your v6 enabled competition and sue you
4. Regulators begin sending greetings …

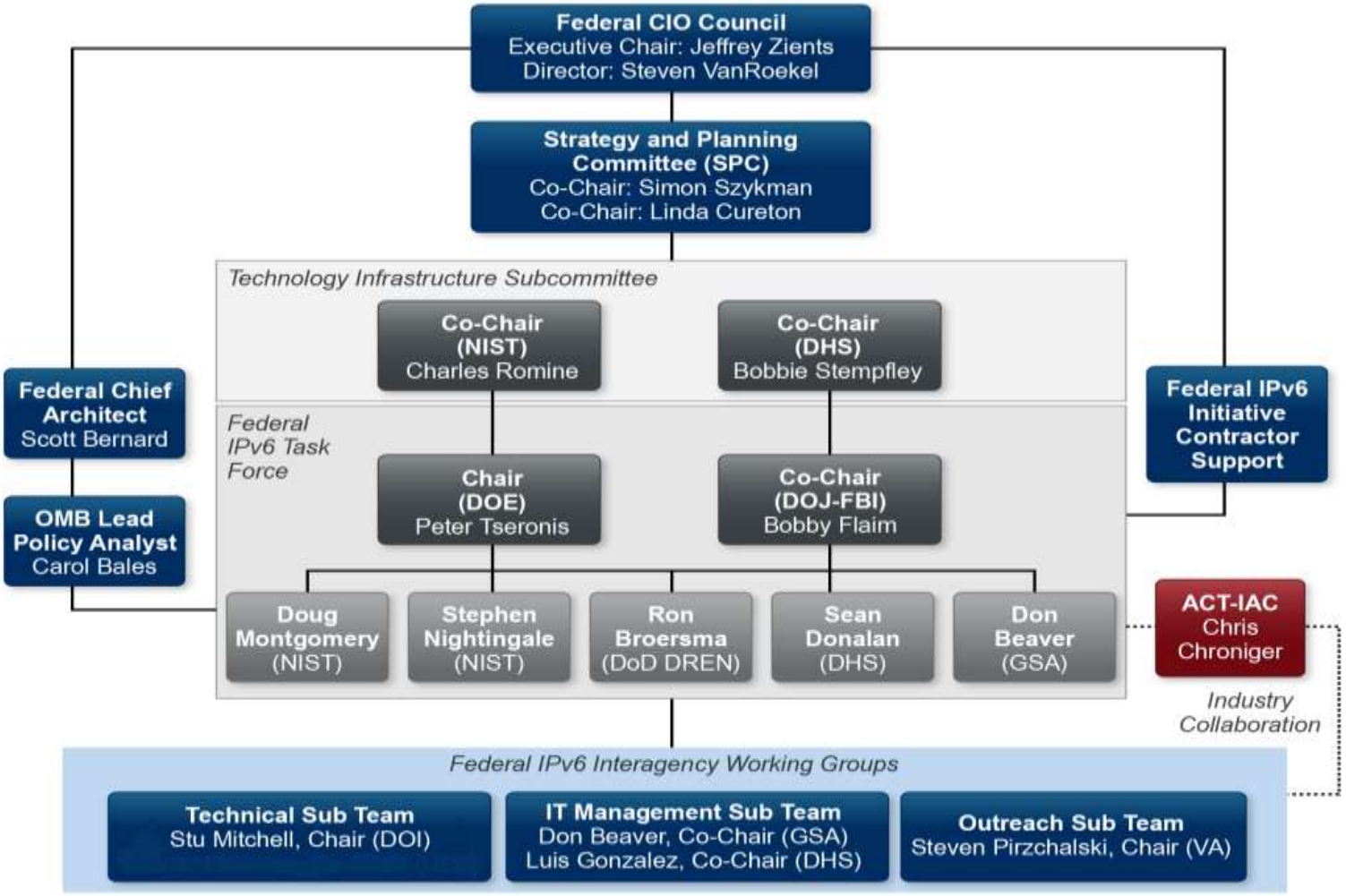

Team Members

Agency Wide Cross Functional Teams

Cross Functional Team Members

- Executive Management
- Required Sponsor(s)
- Business and Product Management
- Network, Servers and “IT” Technical
- Deployment, Security and Network Management

Federal IPv6 Task Force



- is a non-profit, public-private partnership dedicated to improving government through the application of information technology. ACT-IAC provides an objective, ethical and trusted forum where government and industry exchange information and collaborate on technology issues in the public sector
- Networks & Telecommunications SIG
  - IPv6 Working Group
    - Address Management
    - Project Plan
    - Security


IPv6 Strategies

Shrinking Resources

This is not your fathers v4 network …

Do not apply v4 thinking and design constraints to v6 networks

Ron Broersma, DREN Chief Engineer

Some USG IPv6 Strategies

- Incremental costs for v6 deployment – this is a funded initiative
  - Federal Acquisition Regulations (FAR)
  - Federal Enterprise Architecture (FEA)
  - Sustainment and Technology refresh dollars
- Conformance Testing
- Integration with other CIO/IT initiatives
  - Integral to ***Digital Government***
  - DNSSEC, Trusted Internet Connection (TIC)

Procurement Requirements

- FAR 7.105(b)(4)

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

- FAR 11.002(g)

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

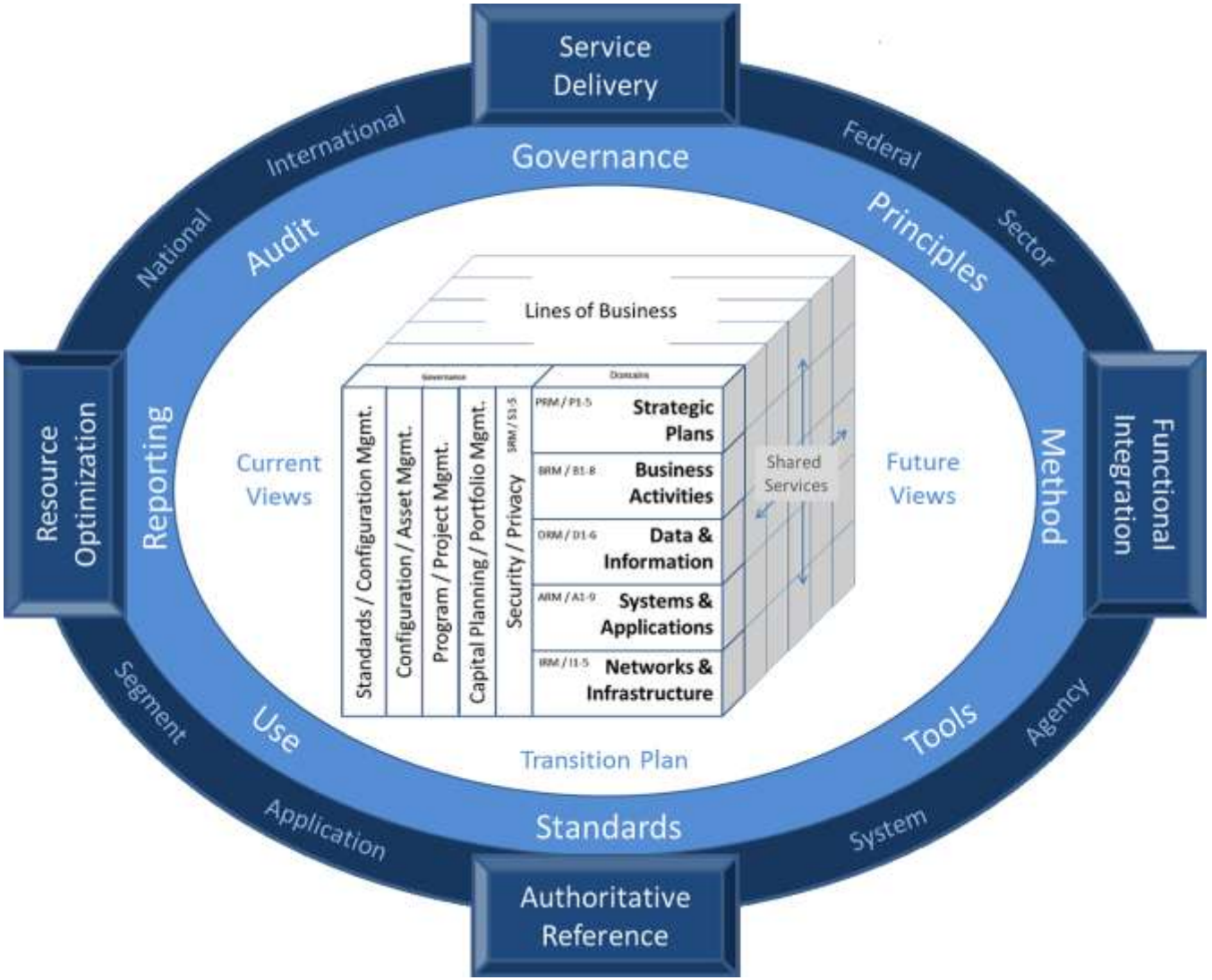
- FAR 12.202(e)

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

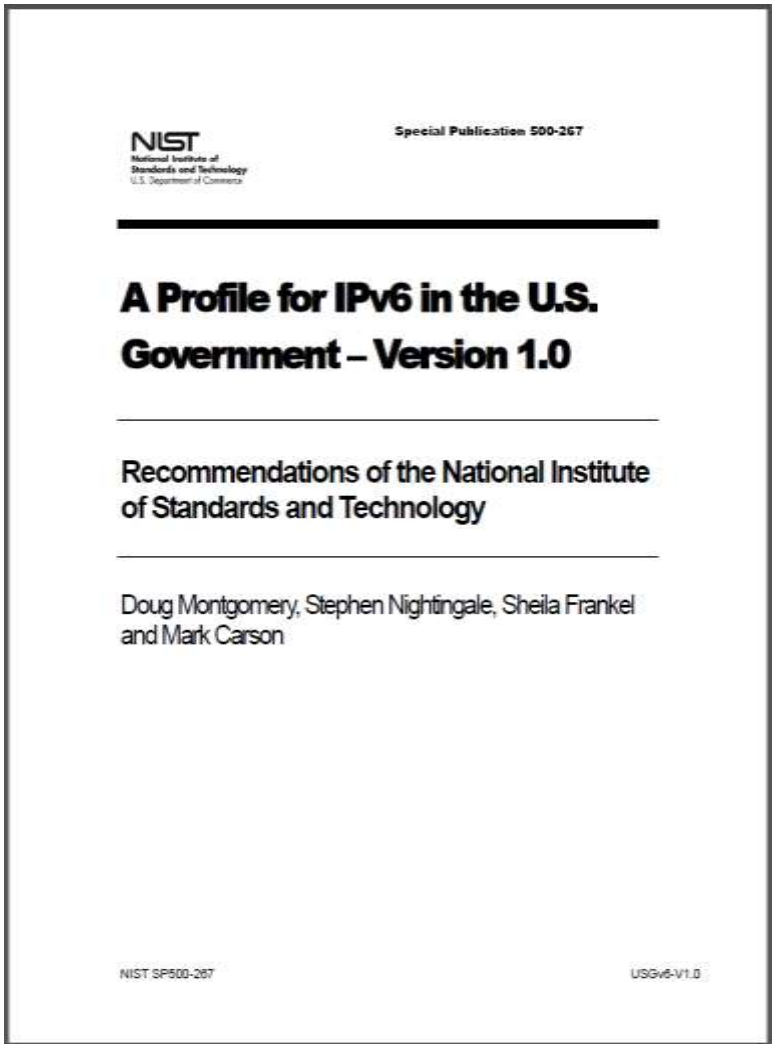
- FAR 39.101(e)

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

Federal Enterprise Architecture Framework II



Product Profile



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

Special Publication 500-267

A Profile for IPv6 in the U.S. Government – Version 1.0

Recommendations of the National Institute of Standards and Technology

Doug Montgomery, Stephen Nightingale, Sheila Frankel and Mark Carson

Supplier Declaration of Comformity

A Profile for IPv6 in the U.S. Government – Version 1.0

Spec / Reference	Section	USGv6-V1 Node Requirements Title / Definition	Status	Year	Condition / Context	Host	Router	NPD	Effective Date
		IPv6 Basic Requirements							
RFC2460		**IPv6 Specification**	DS	1998		**M**	**M**		2010/07
	2	IPv6 Packets: send, receive				**M**	**M**		2010/07
	2	IPv6 packet forwarding					**M**		2010/07
	4	Extension headers: processing				**M**	**M**		2010/07
	4.3	Hop-by-Hop & unrecognized options				**M**	**M**		2010/07
	4.5	Fragment headers: send, receive, process				**M**	**M**		2010/07
	4.6	Destination Options extensions				**M**	**M**		2010/07
RFC5095		**Deprecation of Type 0 Routing Headers**	PS	2007		**M**	**M**		2010/07
RFC2711		**IPv6 Router Alert Option**	PS	1999			**M**		2010/07
RFC4443		**ICMPv6**	DS	2006		**M**	**M**		2010/07
RFC4884		**Extended ICMP for Multi-Part Messages**	PS	2007		S+	S+		
RFC1981		**Path MTU Discovery for IPv6**	DS	1996		**M**	**M**		2010/07
	4	Discovery Protocol Requirements				**M**	S+		2010/07
RFC2675		**IPv6 Jumbograms**	PS	1999		O	O		
RFC4861		**Neighbor Discovery for IPv6**	DS	2006		**M**	**M**		2010/07
	4.1, 4.2	Router Discovery				**M**	**M**		2010/07
	4.6.2	Prefix Discovery				**M**	**M**		2010/07
	7.2	Address Resolution				**M**	**M**		2010/07
	7.2.5	NA and NS processing				**M**	**M**		2010/07
(RFC4862)	7.2.3	Duplicate Address Detection				**M**	**M**		2010/07
	7.3	Neighbor Unreachability Detection				**M**	**M**		2010/07
	8	Redirect functionality				S	**M**		2010/07
RFC5175		**IPv6 Router Advertisement Flags Option**	PS	2008		S	S		
RFC4191		**Default Router Preference**	PS	2005		S+	S+		
RFC3971		**Secure Neighbor Discovery**	PS	2005	SEND	c(M)	c(M)		2010/07

Federal CIO Initiatives

- Digital Government -Building a 21st Century Platform to Better Serve the American People
- IT Modernization, USG Configuration Baseline, HSPD-12 (Secure ID)
- Cloud Computing: Cloud First Strategy
- Federal Data Center Consolidation Initiative (FDCCI)
  - Server, Appliance or Virtual Machine

USG IPv6 Timeline

- 1994 Forward - USG involved in Next Gen Network
- Oct. 2003 - DoD mandates IPv6
- August 2005 - Memorandum M-05-22, “Transition Planning for Internet Protocol Version 6 (IPv6)” (June 2008)
- June 2008 - IPv6 traffic passed on USG backbones
- May 2009 - Initial release of Roadmap Document
- Dec. 2009 - FAR IPv6 regulations go into affect
- Sept. 2010 - OMB Memo on “Transition to IPv6”
- July 2012 - Version 2.0 Roadmap Document Released
- Sept. 2012 - 35% of USG Domains
- Sept. 2014 - Internal networks use v6 for external access
- Sept. 2016 - Planned IPv4 Protocol Decommission

Network Reliability Categories

- National Command Authority
- Life Safety — FAA, Medical, Fire, Police
- Service Provider — 5,000 - 10,000
- Enterprise — 100 - 1,000
- “Home” or Subscriber — 1 - 10

- Service Provider Network Requirements
  - Designed, Tested, Provisioned, Deployed, Secured and Monitored
  - Integrated, Automated systems
  - Two vendor policy for devices, network services (DNS, DHCP, AAA), software and circuits

Federal CIO Initiatives …

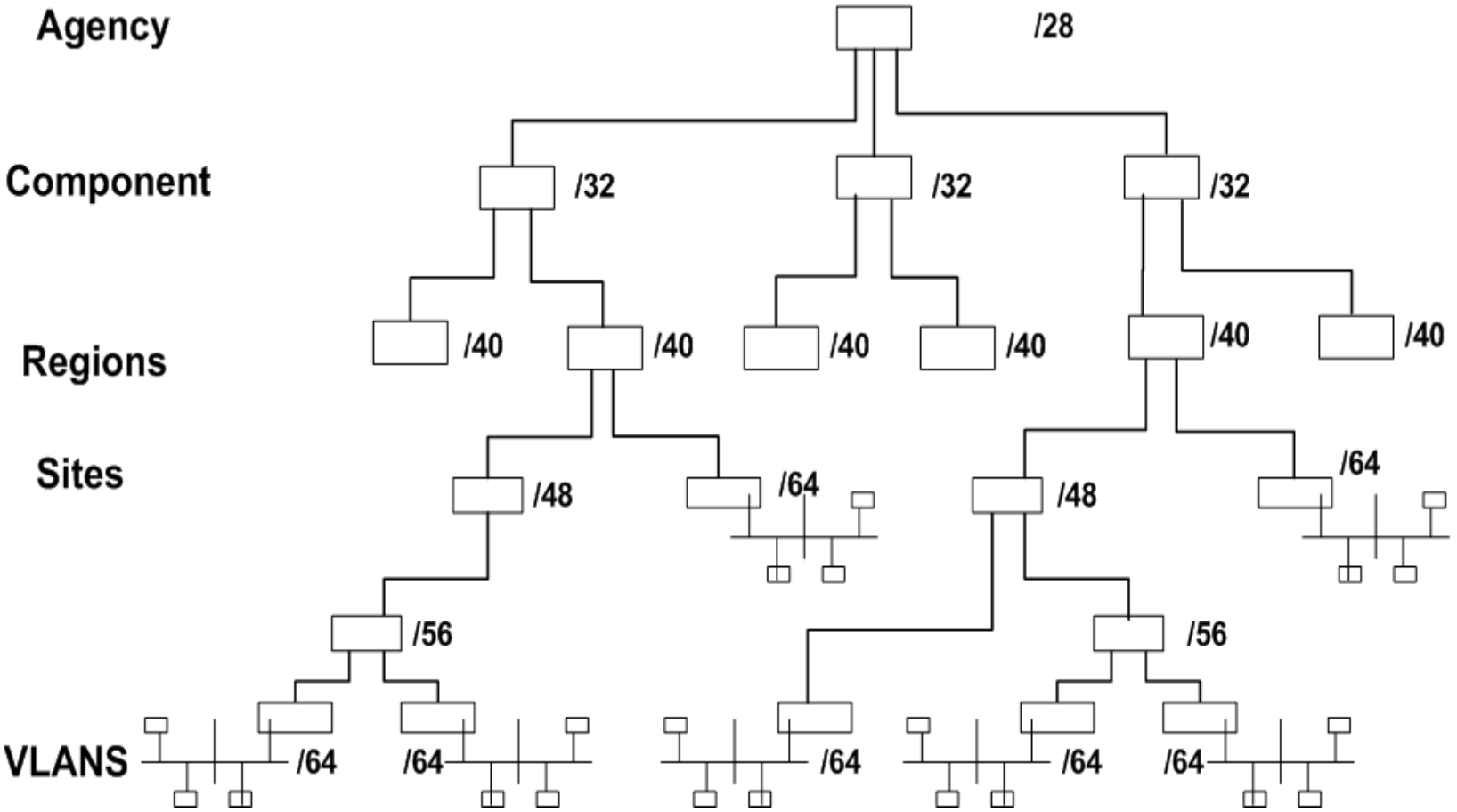
- 2012 Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government
  - Supports a Central Addressing Authority
  - Secure Network wide Access
  - Automated IP Address Planning, Design, Management and Deployment
  - Multi-vendor DNS, DHCP AND AAA
    - Auto generation of A, AAAA and reverse zone RR


Transition Steps

Transition Steps

- Implement a new or utilize an existing Test Lab
  - Same vendor's equipment and configurations
- Standup A Centralized Addressing Authority
  - Promulgate address policies and coordinates with RIR, external and internal stake holders
  - Standard block allocation sizes
  - Exception policy support (nonstandard request)
  - Automated tool with standard interfaces
  - Reporting into CXO level

Address Space Plan



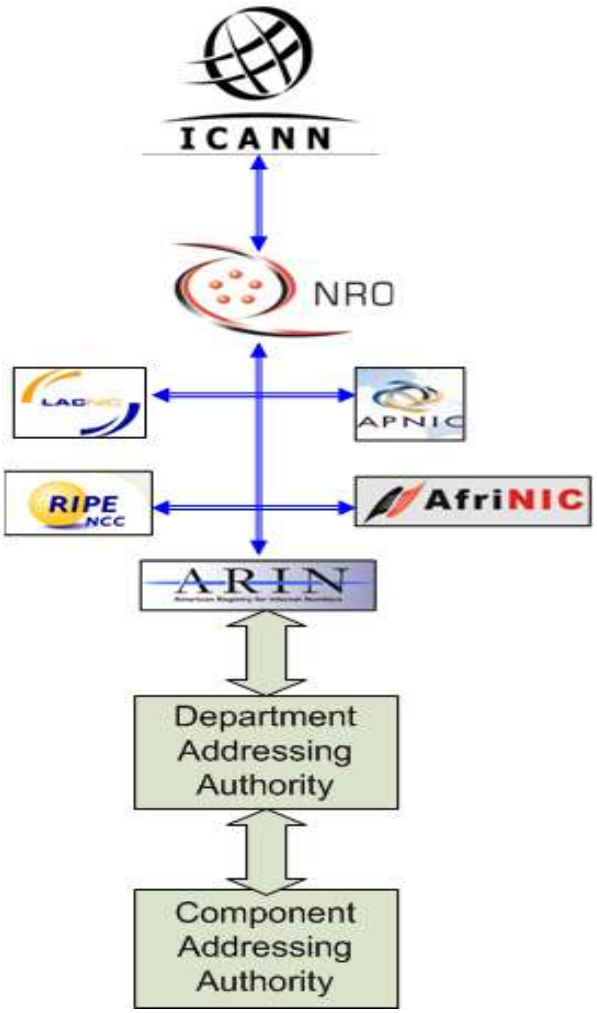
- Address Plan Management and Policies
- Acquire Address block
  - Add up all v4 space including duplicate RFC1918
  - Run Table top exercises to validate hierarchical levels and expansion requirements per level
- Address Space Plan Management and Address Assignment System

- Interfaces for DHCP, DNS, Network Provisioning and Management Systems
- Domain Name Services (DNS) and DNSSEC
- Address Assignment Methods
- Network Management

- Network Device Configuration Management Systems
- Network Engineers, Operations and Management Systems

Management of Address Plan

- Ascertain address needs
- Obtain sufficient address blocks for planning horizon
- Establish Management & allocation policies
  - Standard allocation sizes
  - Exception requests
- Address coordination through accessible repository



Network and Cyber Security

- Threats and Attacks Analysis
- IPv6 Capable Network and Security Devices

What are the Threats?

http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

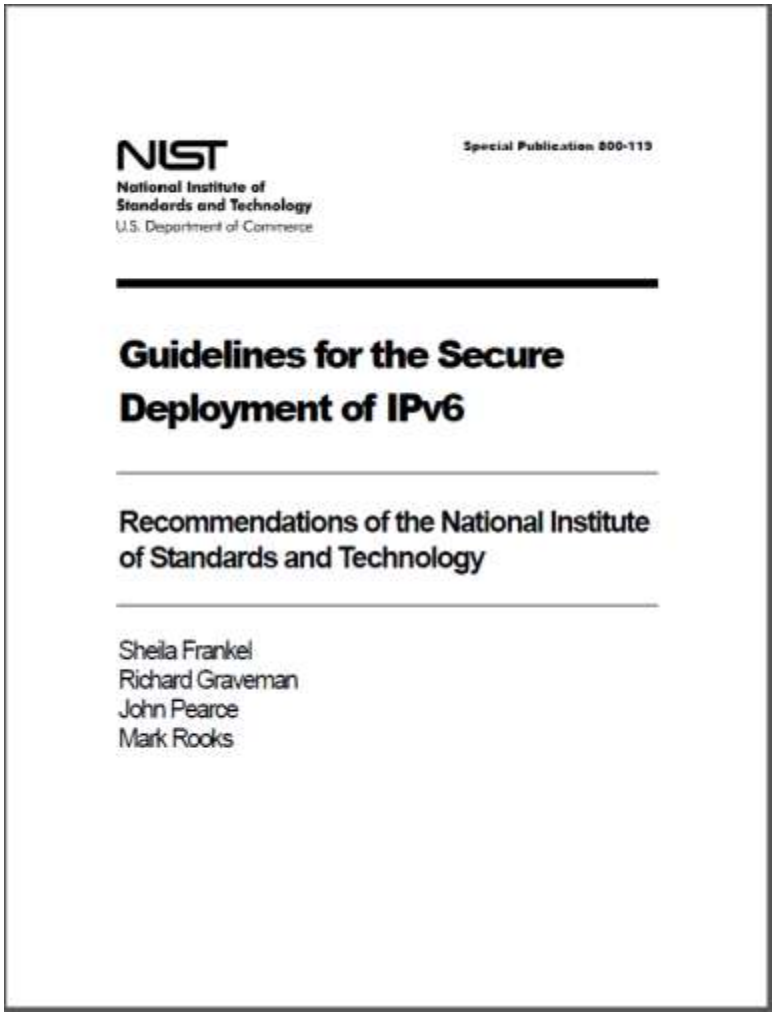
Characteristics of the attacks (2012 Numbers)

- Who is behind the data breaches?
  - 98% Stemmed from external agents (+6%)
  - 4% Implicated insiders (-13%)
  - 58% of all data thefts tied to activist groups
- How do breaches occur?
  - 81% Utilized some form of hacking (+31%)
  - 69% Incorporated malware (+20%)
  - 10% Involved physical attacks (-19%)
  - 7% Social tactics / engineering (-12%)
  - 5% Resulted from privilege misuse (-12%)

What Commonalities Exist

- 79% of victims were targets of opportunity (-4%)
- 96% of attacks were not highly difficult (+4%)
- 94% of all data compromised involved servers (+18%)
- **85% of breaches took weeks or more to discover** (+6%)
- **97% of breaches were avoidable through simple or intermediate controls** (+1%)
- 96% of victims subject to PCI-DSS had not achieved compliance (+7%)

Secure Deployment of IPv6



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

Special Publication 800-119

Guidelines for the Secure Deployment of IPv6

Recommendations of the National Institute of Standards and Technology

Sheila Frankel
Richard Graveman
John Pearce
Mark Rooks

Defense in Depth IPv6 & v4

- Personnel education and training
  - Password security
  - Phishing and other social engineering attacks
    - Facebook and other networking sites
- Perimeter and security enclave defenses
  - Firewalls, IDS/IPS, Honey pots, Router & Switch ACLs, Proxies, Deep Packet Inspect
- Server/client behavior analysis within enterprise i.e. a client should not start scanning addresses or serving content

Attack Mitigation Strategies

- Ensure essential controls are in place and regularly checked
- Event and system logs are regularly monitored and mined to proactively identify problems
- Do not encode Information in the Interface ID

Device and Network Discovery

- Certify, provision and rollout systems onto the network
  - Do not *discover uncertified or untested systems* and automatically ad them to the network
  - Implement Network Access Controls
- Any unauthorized devices discovered should be considered hostile

Management & Pivot Systems

- Productive Attack Vectors
  - Network Provisioning, Operations & Management Systems
  - Address Management, DNS, DHCP, AAA
  - Network Engineers systems used for configuration, monitoring and management
    - Only attached to the Network under management with cryptographic methods

Targets of Opportunity

- Network Engineering and operations personnel should have clean, single purposes systems for network, operations & security management.
  - No un-encrypted Internet Access
  - All unused applications and services turned off
- Out of band management networks
- Address planning and management systems behind firewalls and not widely connected to the edge or Internet facing networks


Take Aways

- Inventory, assess, analyze and plan now
- Develop the cost models and other resource requirements
- Start with outward facing servers and services
- Kick off the project:
  - when business conditions are met, specific customer needs,
  - Other internal projects that can be transitioned early or as part another project

- How mission critical is your network and design it accordingly. Power, HVAC, interconnectivity, backup services …

Resources

- Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government
  - https://cio.gov/wp-content/uploads/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf
- Digital Government Initiative
  - http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

Industry Contributors

Chris Chroniger – Chair	Acentia
Dale Geesey	Auspex Technologies
Kenny Burroughs	Internet Associates
Barry Chapman	Acentia
Jeremy Duncan	Salient Federal
TJ Evans	Nephos6
Joe Klein	QinetiQ, North America
Tim Owen	SMS
Chip Popoviciu	Nephos6
Yanick Pouffary	HP
Yurie Rich	Nephos6
Kristofer Smith	Auspex Technologies
Frank Troy	Troy Networks
Ralph Wallace	White Oak Consulting

Contact Information

- John L. Lee, CTO
  - john@internetassociatesllc.com
    +1-678-488-6085
- Internet Associates, LLC
  - +1-855-GET-IPV6
    +1-770-495-0953