

# Why Are We Here?

## Identifying and Removing Barriers to IPv6 Deployment

**Doug Montgomery (dougmont@nist.gov)**

# USG strategic commitment to IPv6

- **Motivations:**

- Foster USG adoption of IPv6 as enabling technology for IT modernization.
- Support USG initiatives in cloud, virtualization, mobility, IoT, transportation, public safety.
- Reduce complexity and improve the security of USG network infrastructures.
- Serve as a catalyst to the IPv6 industry.

- **Actions:**

- Establish standards and testing to protect USG investments in IPv6 technology.
- Develop security guidance for the IPv6 deployment.
- Promulgate acquisition and deployment polices to achieve objectives.

# Federal IPv6 Initiatives

## • Federal IPv6 Initiative

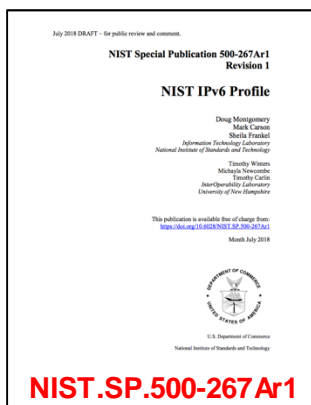
- 2005 - Transition Planning for Internet Protocol Version 6 (IPv6): Memorandum for The Chief Information Officers. [OMB-M05-22]
  - **Instructs agencies to plan for IPv6 transition and enable WAN capabilities.**
  - **Instructs NIST to develop standards and testing to facilitate USG adoption of IPv6.**
- 2008 - A Profile for IPv6 in the U.S. Government. [[SP500-267](#)]
- 2008 - MOU between NIST and the IPv6 Forum. [[NIST-IPv6F](#)].
- 2009 - IPv6 Test Methods: General Description & Validation. [[SP500-273](#)]
- 2009 - Federal Acquisition Regulation: FAR Case 2005-041, IPv6. [[FAR-2005-041](#)]
- 2010 - Guidelines for the Secure Deployment of IPv6. [[SP800-119](#)]
- 2010 - Transition to IPv6: Memorandum for Chief Information Officers of Executive Departments and Agencies. [[OMB-IPv6](#)]
  - **2012 – IPv6 Enable publicly accessible Internet services.**
  - **2014 – IPv6 Enable enterprise networks.**

# USGv6 Program

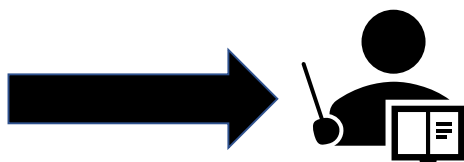
## • USGv6 Profile ~2008

- Supports both the specification of IPv6 acquisition requirements and the testing of commercial products.
- Establishes a vocabulary for stating requirements and describing product capabilities.
- Fill gaps in industry standards – mainly in developing requirements for FW/IDS.

### Standards Profile



### User / System Requirements



### Procurement Requirements

Agency-Default-Server=NISTv6-r1:Host+Core+SLAAC  
+Addr-Arch+Multicast+[IPsec][TLS]+DHCP-Client+URI+DNS-Client+Link=Ethernet



### IPv6 Capable Product



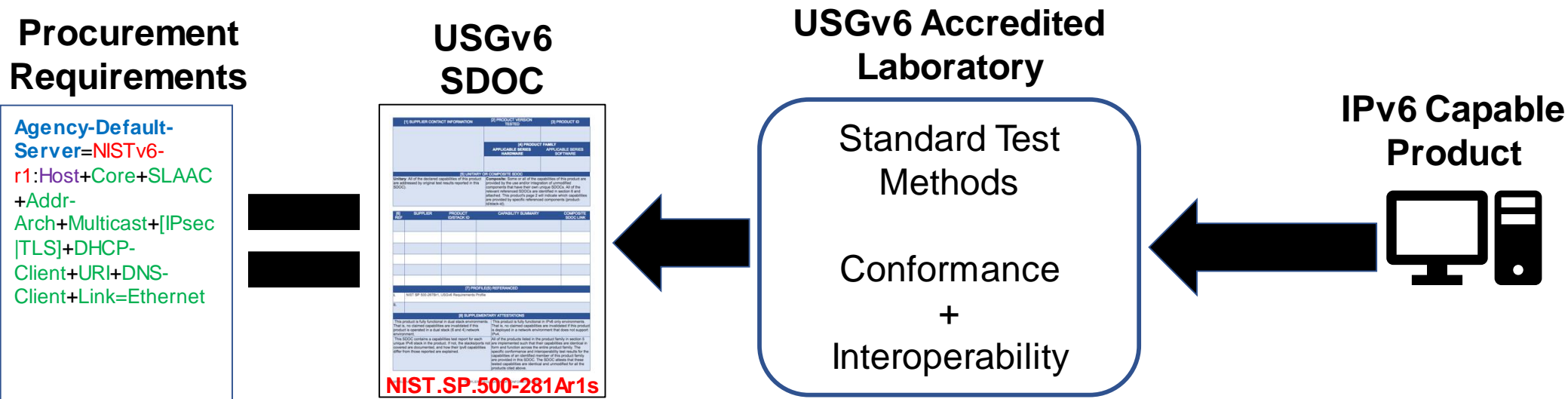
# USGv6 Testing Program

- **USGv6 Test Program committed to converge / harmonize**

- IPv6 Ready Logo Test Specifications
  - NIST and IPv6 Forum sign MOU
- DoD Generic Test Plan test cases



- Claims of compliance shall be documented using Supplier's Declaration of Conformity (SDoC)



# USGv6 Testing Program

## • USGv6 Tested Product List

- <https://www.iol.unh.edu/registry/usgv6>
- Hosts Tested (298)
- Routers Tested (142)
- NPDs Tested (34)
- ~1400 products tested for USGv6
  - Over 10,000 products listed.

## • USGv6 Program

- <https://www.nist.gov/programs-projects/usgv6-program>
- **New revisions of USGv6 Profile & Test Program specifications out for comment.**



University of New Hampshire  
InterOperability  
Laboratory

Company	Product Name	Type	Version Tested	Hardware	Software	Test Suites	SDoc
Cisco Systems	Cisco ATA 191 Analog Telephone Adapter	Host	12.0(1)SR1	• ATA 191 Analog Telephone Adapter	12.0(1)SR1	<ul style="list-style-type: none"> <li>• Basic Interoperability v1.1 (29915)</li> <li>• Basic Conformance v1.2 (29913)</li> <li>• SLAAC Interoperability v1.2 (29915)</li> <li>• SLAAC Conformance v1.1 (29913)</li> <li>• Addr Arch Interoperability v1.1 (29914)</li> <li>• Addr Arch Conformance v1.2 (29912)</li> </ul>	View
Riverbed Technology, Inc.	Riverbed SteelFusion	Host	6.0.0	<ul style="list-style-type: none"> <li>• SteelFusion Core: SteelFusion Core 3500</li> <li>• SteelFusion Edge: SteelFusion Edge 2100, SteelFusion Edge 2200, SteelFusion Edge 3100, SteelFusion Edge 3200, SteelFusion Edge 5100</li> </ul>	Virtual SteelFusion Core 6.0 Virtual SteelFusion Edge 6.0	<ul style="list-style-type: none"> <li>• Basic Interoperability v1.1 (29579)</li> <li>• Basic Conformance v1.2 (29577)</li> <li>• SLAAC Interoperability v1.2 (29579)</li> <li>• SLAAC Conformance v1.1 (29577)</li> <li>• Addr Arch Interoperability v1.1 (29580)</li> <li>• Addr Arch Conformance v1.2 (29578)</li> </ul>	View
Microsoft Corporation	Windows Server	Host	Windows 2016 Server		Windows 2016 Server and all versions of Windows based on the Windows Server stack without any significant changes that would affect the performance of the IPv6 stack.	<ul style="list-style-type: none"> <li>• Basic Interoperability v1.1 (29787)</li> <li>• Basic Conformance v1.2 (29786)</li> <li>• SLAAC Interoperability v1.2 (29787)</li> <li>• SLAAC Conformance v1.1 (29786)</li> <li>• Addr Arch Interoperability v1.1 (29789)</li> <li>• Addr Arch Conformance v1.2 (29788)</li> </ul>	View

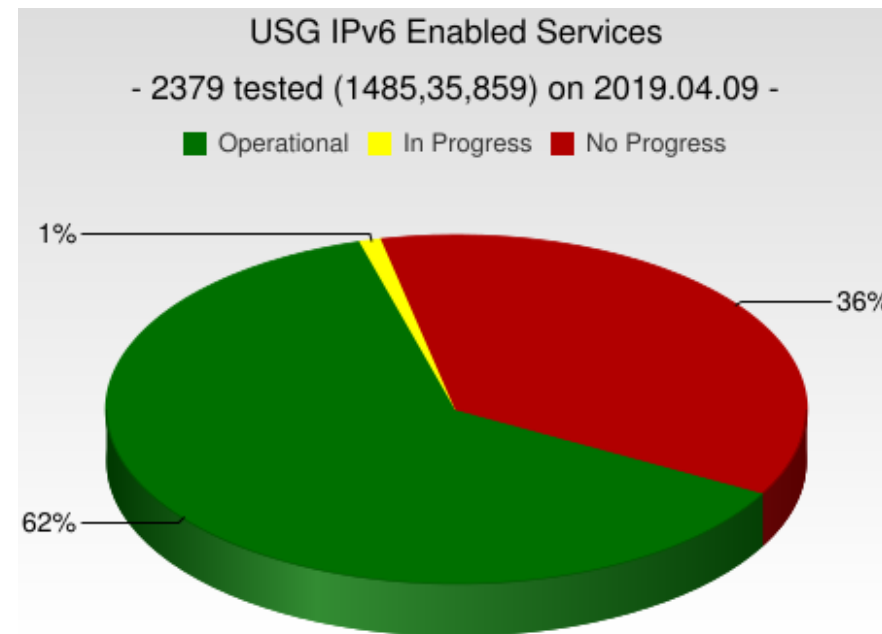
# USG Internet Facing Public Services

- **Milestone**

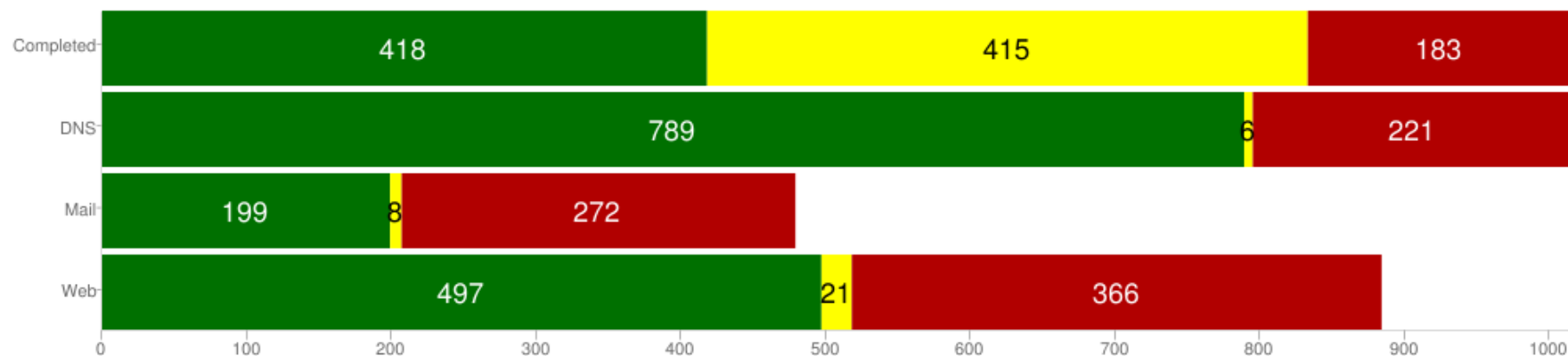
- 62% Complete →

- **Service Level Details**

- DNS 78%
- Email 41%
- WWW 56%



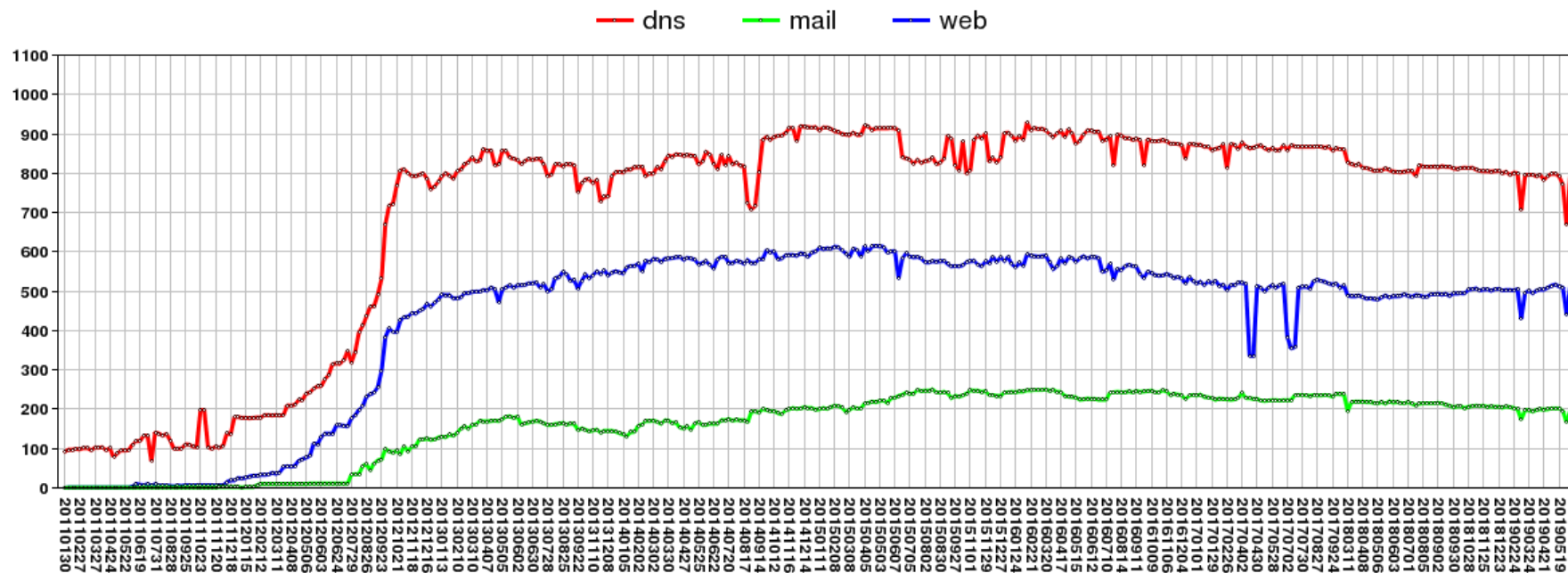
USG IPv6 Enabled Domains  
- 1016 tested on 2019.04.09 -



# Completing the USG transition to IPv6

- **USG progress has plateaued in recent years.**
  - Enterprise deployment is lagging.
- **Identify and address barriers to achieving**
  - IPv6-Everywhere
  - IPv6-Only

USG IPv6 Operational Service Domains Over Time





# USG challenges going forward

- **Much has changed since 2005 – 2010, we need to:**
  - better articulate business case, not just policy mandates;
  - foster commercial products capable of IPv6-only operation;
  - evolve focus of transition technologies from IPv6 bootstrap, to legacy IPv4 interoperability;
  - demonstrate and document playbooks for real-world deployment scenarios using commercial equipment;
  - ensure that leading edge security technologies / architectures are IPv6-capable; and,
  - demonstrate new capabilities enabled by IPv6, beyond bigger addresses.

# Industry taking the lead on IPv6 adoption

- **Recent Progress in Some Areas**
- In the last 5 years, IPv6 momentum in industry has dramatically increased, with large commercial IPv6 deployments in several industry sectors (e.g., data centers, cellular carriers, content providers) now driven by business goals of reducing cost, decreasing complexity, improving security and eliminating barriers to innovation in networked information systems.
  - **State of IPv6 Deployment, Internet Society,**  
<https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/>
  - **Case Study: Facebook Moving To An IPv6-Only Internal Network,**  
<https://www.internetsociety.org/resources/deploy360/2014/case-study-facebook-moving-to-an-ipv6-only-internal-network/>
  - **Case Study: T-Mobile US Goes IPv6-only Using 464XLAT,**  
<https://www.internetsociety.org/resources/deploy360/2014/case-study-t-mobile-us-goes-ipv6-only-using-464xlat/>

# Enterprise Deployment Lagging

- **Widescale adoption in \ enterprise settings continues to lag.**
  - Significant potential benefits to transitioning enterprise networks to IPv6, but questions remain about the viability of security and transition technologies and deployment guidance necessary to do so safely.
  - **Case Study: Microsoft Works Toward IPv6-Only Single Stack Network,**
    - <https://teamarin.net/2019/04/03/microsoft-works-toward-ipv6-only-single-stack-network/>
- **What are the barriers to enterprise deployment?**
  - Business Case –
  - Technology –
  - Products / Services –
  - Knowledge Base –
  - Operational Issues -

# Security for IPv6 Enabled Enterprises

- ***Focus of the workshop and subsequent NCCoE project:***
  - Examine the extent to which current commercially available security technologies can support wide scale deployment of IPv6 in a range of enterprise use case scenarios.
- ***Enterprise security technologies to be considered include:***
  - identity and access management systems;
  - access control and policy enforcement systems, threat intelligence and reputation systems;
  - virtual private networks and remote access technologies;
  - firewalls and intrusion detection / protection systems, end-point security systems;
  - security incident and event management systems; and,
  - core network infrastructure systems (e.g., switching, routing, naming) and associated monitoring and management systems.
- ***Enterprise use cases to be considered include:***
  - desktop to on premise service access; enterprise access to cloud-based services; and, remote access to enterprise services.

# Security for IPv6 Enabled Enterprises

- **A second focus of the workshop and subsequent planned NCCoE project is to examine the state of existing standards, guidance and industry best practice documentation.**
  - to demonstrate the viability of implementing such specifications with commercially available products; and,
  - to identify gaps in the knowledgebase that should be filled with additional guidance and specifications.
- **The proof-of-concept demonstration project will exercise existing guidance from NIST and the Internet Engineering Task Force .**
  - It is anticipated that the outcome of the project will inform updates to the NIST guidelines and recommendations.
    - Guidelines for the Secure Deployment of IPv6, <https://csrc.nist.gov/publications/detail/sp/800-119/final>
    - IETF IPv6 Operations Working Group, <https://datatracker.ietf.org/wg/v6ops/documents/>
    - IETF Operational Security Capabilities for IP Network Infrastructure Working Group, <https://datatracker.ietf.org/wg/opsec/documents/>

# Our plan for today!

09:00 – 09:15	Welcome & Introduction to NCCoE Kevin Stine, NIST
09:15 – 09:30	Identifying and Removing Barrier to IPv6 Development Doug Montgomery, NIST
09:30 – 10:45	Enterprise Challenges <ul style="list-style-type: none"> <li>IPv6 Motivations and Obstacles Lee Howard, Retevia</li> <li>IPv6 Adoption at a Large Enterprise John Burns, Wells Fargo</li> </ul>
10:45 – 11:00	BREAK
11:00 – 12:00	Enterprise Challenges <ul style="list-style-type: none"> <li>Microsoft Corporate Network: Journey to IPv6 Dawn Bedard, Microsoft</li> <li>DoD IPv6 Context and Way Ahead Col. Keith Repik, DoD</li> </ul>
12:00 – 12:15	BREAK
12:15 – 1:00	Breakout Sessions – Identifying Barriers to Deployment Participants will break into groups of 8-10
1:00 – 1:30	Readout, Discussion and Next Steps
1:30	Formal Program Concludes
2:30-3:30	*Optional: Informal Discussions with NCCoE Regarding Potential Project Scoping and Collaborations

## • We want your input!

- ~125 organizations registered
- Industry sectors
- Professional roles
- Levels of IPv6 experience
  - From: “haven’t started business case” to
  - To: “full enterprise IPv6 deployment”.

# Identifying Barriers to IPv6 Enterprise Adoption

- **Organize into breakout groups.**
  - 6 breakout groups & facilitators.
    - Count off 1,2,3,4,5,6 ....
  - Contribute your experience / perception of the barriers to IPv6 adoption.
    - Equally important: contribute your ideas of practical actions that could remove these barriers.
    - If possible, roughly group by priority.
  - All input will be shared without attribution (person or affiliation).
    - We want your personal experience.
- **Objective: Identify Barriers**
  - **Discuss two contexts:**
    - **IPv6-Everywhere** – getting to ubiquitous deployment and use of IPv6 as the dominant / preferred protocol.
    - **IPv6-Only** – removing IPv4 support from segments of the enterprise.
  - **Categorize Barriers and Gaps**
    - Business Case –
    - Technology –
    - Products / Services –
    - Knowledge Base –
    - Operational Issues -

# Questions / issues to consider

## • Level setting your perspective

- Your industry sector & size?
- Where is your organization WRT IPv6?
  - No activity.
  - Establishing the business case.
  - Planning / testbed pilots.
  - Some operational dual-stack deployment.
  - Full / mature operational dual-stack deployment.
    - “IPv6-Everywhere”
- “IPv6-Only”?
  - Similar questions to above.

## • Business Case

- Understanding cost / ROI.
  - Near term & long term
- Technical motivation
  - Innovation, beyond more addresses!
- Security motivation
  - How IPv6 improves security / robustness

## • Technology

- Unsolved issues in IPv6
  - Need for standards / specifications?
- Technical issues in IPv6
  - Challenges presented by IPv6 design?
- Transition Technologies
  - Challenges presented by IPv4 interop?



# Questions / issues to consider

## • Products and services

- Availability of IPv6 products?
  - Gaps in offerings?
- Completeness of IPv6 products?
  - Feature parity with IPv4?
  - Capable of IPv6-Only operation?
- Quality of IPv6 products?
  - Conformance / interoperability?
  - Scalability / robustness?
- How are issues different with:
  - Hosts / OSs
  - Routers / switches
  - Cloud services

## • Security products / services

- Identity and access management systems;
- Access control and policy enforcement systems, threat intelligence and reputation systems;
- Virtual private networks and remote access technologies;
- Firewalls and intrusion detection / protection systems, end-point security systems;
- Security incident and event management systems; and,
- Monitoring, mitigation and management systems.

# Questions / issues to consider

## • Knowledge Base

- General training & information?
- Deployment & operation guidance?
- Security guidance?
- Documented example deployments and detailed “playbooks”?

## • Operational Issues

- Challenges posed IPv6 operation?
  - Challenges specific to dual-stack?
  - Challenges specific to IPv6-only?
- Monitoring and management?
- DevOps / automation?

## • Breakout group report

- Facilitator will report for group.
- Summarize common / salient points.
  - Roughly group/prioritize if possible.
- Remember to include suggestions for addressing barriers.

## • Next Steps

- Develop workshop report white paper.
- NIST/NCCoE develop project plan for collaborative demonstration projects.