Embracing IPv6 in Federal Acquisition

Stephen Nightingale, NIST

October 12, 2011

Overview

- Why transition to IPv6?
- The Issues: Agencies _buying approved IPv6 products_ in a _constrained budget environment_.
- Federal Government Interfaces to USGv6
- IPv6 Acquisition Processes and Procedures
  - What the Buyer should do
  - What the Acquisition official should do
  - Examples: Routers, Firewalls, Laptops, Services
- The Capabilities Checklist
- Next Steps
- Resources

Why we must transition to IPv6

- The federal government must transition to IPv6 to 'future proof' its services to the Public.
  - The available pool of IPv4 addresses was recently exhausted – impacting anything that needs an IP address.
  - Government services must be available to members of the public and customers who have IPv6 only access. (They need to reach us, and we need to reach them).
  - IPv6 will ensure the successful deployment and expansion of IT modernization initiatives, such as cloud computing, smart-grid.
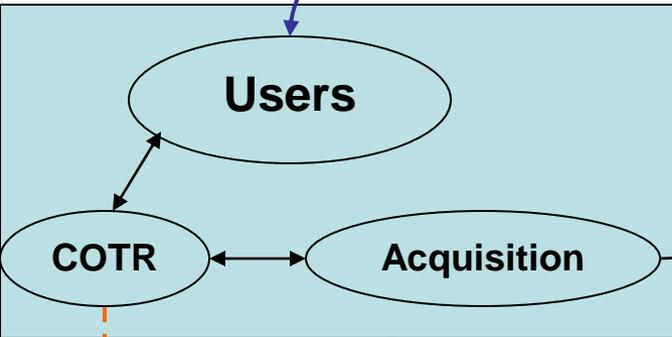
The Issues

- How can we permeate across all federal agencies the know-how to ensure they are buying IT products with USGv6 capabilities, in a simplified and unified manner?

- How can we ensure that IPv6 rollout proceeds in an era of severe Agency belt-tightening?
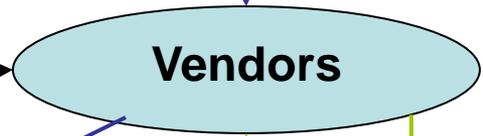
Federal Government Interfaces to USGv6

- **IPv6 Interagency Group** and governance structure.
- **FAR clause**: for Buyers and Acquisition Officials
- **USGv6 Profile**: full technical specification of IPv6 capabilities for networked IT products
- **USGv6 Capabilities**: summary expression of buyers needs.
- **SDOC (Suppliers Declaration of Conformity):** expression of product testing results.
- **USGv6 Website**: advice for all stakeholders.

USGv6 Profile

Users

COTR ↔ Acquisition

Vendors

RFP

Corroboration

Vendor's SDOC

Test Results

V6 Product

Test Labs
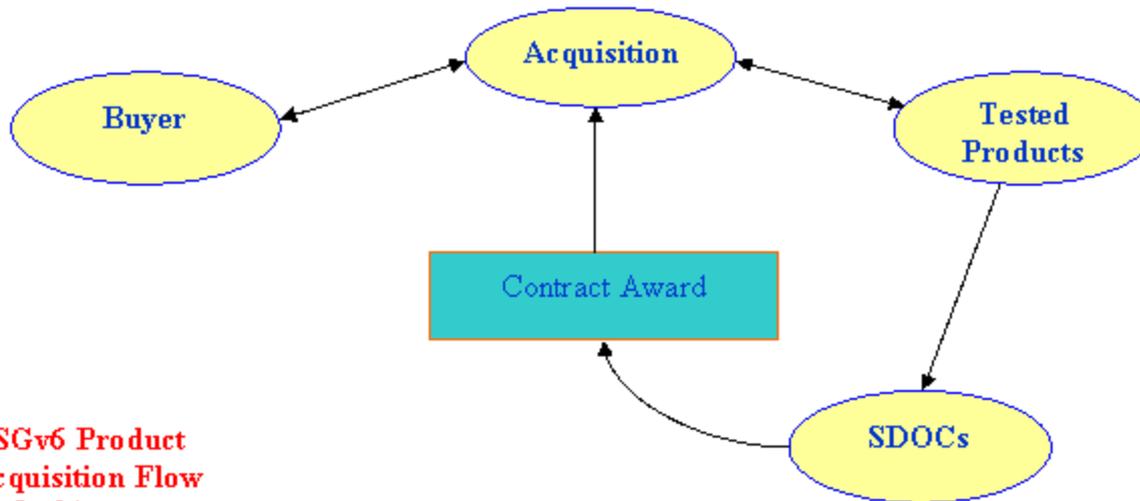
Overall Process: The Acquisition Cycle
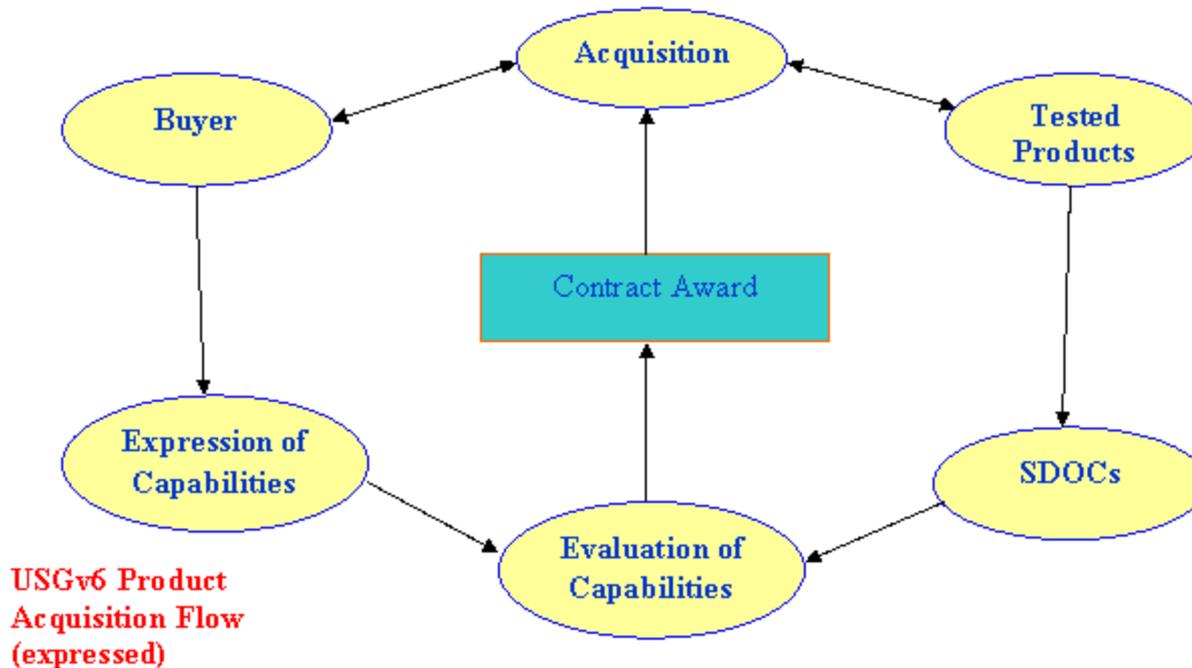
What the Buyer can do (1)

- Default versus expressed acquisitions
  - Default: no need to express capabilities
  - Expressed: tailoring capabilities to local needs and any Agency policy
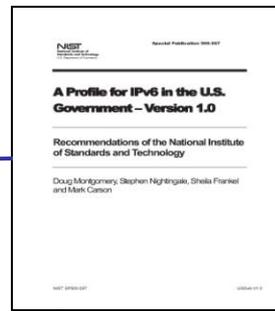

USGv6 Product
Acquisition Flow
(default)

What the Buyer can do (2)

- Large or complex or specified acquisition
  - Networking capabilities are expressed
  - And responses must be evaluated

USGv6 Product
Acquisition Flow
(expressed)
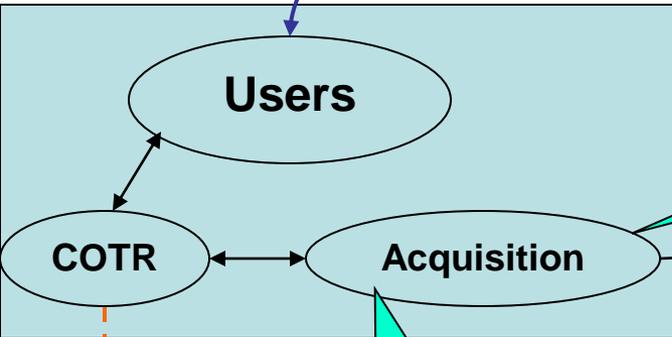
USGv6 Profile

Reflect SDOCs back to buyers

Users

COTR

Acquisition

RFP

Vendors
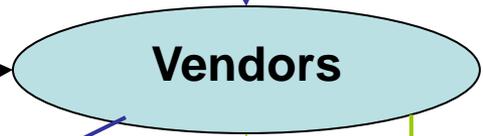
Make sure the FAR is adhered to

Vendor's SDOC

Test Results

V6 Product

Corroboration

Test Labs

What Acquisition can do (1)

USGv6 Profile

Users
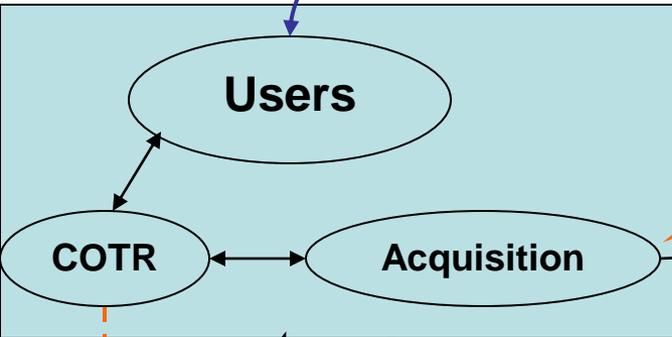
Agency wide training and awareness

Vendors

COTR

Acquisition

RFP

Agency Acquisition Manuals

Vendor's SDOC

Test Results

V6 Product

Corroboration

Test Labs

What Acquisition can do (2)

Some Examples

- ## What Products more likely need technical capabilities expressed?
  - ### Routers
    - You will at least need to specify a routing algorithm.
      - OSPFv3 is the USGv6 recommended default, but your Agency may use something different, such as IS-IS.
  - ### Firewalls
    - You will need to specify whether it must be a simple firewall, or Intrusion Detection or Intrusion Prevention system.

- ## What Products may not need technical capabilities expressed?
  - ### Laptops, Notebooks, IPads
    - However, they <u>must</u> have an SDOC indicating IPv6 support.

CAPABILITIES CHECKLIST: DISCUSSION POINTS

- The Capabilities checklist is found in Appendix A of the USGv6 profile
- The checklist is a summary of NIST recommendations for the 12 Functional Categories
- 'Host' and 'Router' are the categories used by the IETF (in RFC 4294)
  - Vendors may implement different/overlapping capability mixes
  - It is the capabilities that matter, NOT the product "category" label
  - If the product has an IPv6 stack, that stack had better be tested
- Capabilities checklist needs technical assessment (OCIO/COTR)

THE CAPABILITIES CHECKLIST

Spec / Reference	Section	USGv6-V1 Capability Check List / IPv6 Requirements	Configuration Option	Host	Router	NPD	Notes
SP500-267	6.1	**IPv6 Basic Requirements**					
		support of core IPv6 capabilities (IPv6, ICMP, ND, PMTU).					
		support of stateless address auto-configuration	SLAAC				Host:[O:1]
		support of SLAAC privacy extensions.	PrivAddr				
		support of stateful (DHCP) address auto-configuration	DHCP-Client				Host:[O:1]
		support of automated router prefix delegation	DHCP-Prefix				
		support of neighbor discovery security extensions	SEND				
SP500-267	6.6	**Addressing Requirements**					
		support of base IPv6 addressing requirements.					
		Addr: "Scoping, Deprecation, Defaults and Reserved"					
		support of cryptographically generated addresses	CGA				
SP500-267	6.7	**IP Security Requirements**					
		support of the IP security architecture	IPsec-V3				
		support for automated key management	IKEv2				
		support for encapsulating security payloads in IP	ESP				
SP500-267	6.11	**Application Requirements**					
		support of DNS client/resolver functions	DNS-Client				
		support of Socket application program interfaces	SOCK				
		support of IPv6 uniform resource identifiers	URI				
		support of a DNS server application	DNS-Sever				
		support of a DHCP server application	DHCP-Server				
SP500-267	6.2	**Routing Protocol Requirements**					
		support of the intra-domain (interior) routing protocols	IGW				
		support for inter-domain (exterior) routing protocols	EGW				
SP500-267	6.4	**Transition Mechanism Requirements**					
		support of interoperation with IPv4-only systems	IPv4				
		support of tunneling IPv6 over IPv4 MPLS services	6PE				
SP500-267	6.8	**Network Management Requirements**					
		SNMPv3: "Mgmt, Messages, Apps and Security"	SNMP				
SP500-267	6.9	**Multicast Requirements**					
		Mcast: "MLDv2, Unicast, Allocation"					
		full support of multicast communications	SSM				
SP500-267	6.10	**Mobility Requirements**					
		support of mobile IP capability.	MIP				
		support of mobile network capabilities	NEMO				
SP500-267	6.3	**Quality of Service Requirements**					
		support of Differentiated Services capabilities	DS				
			PHB Id				
SP500-267	6.12	**Network Protection Device Requirements**					
		NPD "6.12.3 general requirements"	N1|N2|N3|N4				
		support of basic firewall capabilities	FW				NPD:[O:1]
		support of application firewall capabilities	APFW				NPD:[O:1]
		support of intrusion detection capabilities	IDS				NPD:[O:1]
		support of intrusion protection capabilities	IPS				NPD:[O:1]
SP500-267	6.5	**Link Specific Technologies**					
		support of robust packet compression services	ROHC				
		support of link technology [O:1]	Link=				[O:1]
		(repeat as needed) support of link technology	Link=				

Items in parentheses are a compendium of capabilities more fully expressed in the Node Requirements Table.

Next Steps

- Acquisition Managers and Buyers:
  - Implement processes for all agency IT acquisitions to be in accordance with FAR requirements for IPv6.
  - Ensure Buyers procure products in accordance NIST guidelines for USGv6.
  - Submit feedback and comments on the USGv6 Buyer's Guide:
    - To usgv6-project@nist.gov
    - Ongoing: we want continuous improvement and clarification.
- Budget got your belt in a few extra notches?
  - OMB advice from the start was rollout IPv6 on 'Tech Refresh'.
  - Tech Refresh may be slower next year than last year.
  - Adjust plans to accommodate this reality.

Resources

- FAR amendment for IPv6: for Buyers and Acquisition Officials: http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf

- The Full FAR: https://www.acquisition.gov/far/index.html

- USGv6 Profile: full technical specification of IPv6 capabilities for networked IT products. http://www.antd.nist.gov/usgv6/docs/usgv6-v1.0.pdf

- NIST USGv6 Website: http://www.antd.nist.gov/usgv6/

- USGv6 Capabilities Checklist (Appendix A): http://www.antd.nist.gov/usgv6/docs/usgv6-v1.0.pdf

- Suppliers Declaration of Conformity (SDOC) template: http://www.antd.nist.gov/usgv6/sdoc.html.

FAR Information (IPv6)

- FAR Case 2005-041 Internet Protocol version 6
  http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf
- Affecting CFR Parts 7, 11, 12 and 39
- Require IPv6 Compliant products in all new IT acquisitions using IP
- Effective December 10, 2009
- FAR Part 11.002 amendments:
  - Requirements documents must:
    - Include reference to technical capabilities from the USGv6 Profile, NIST SP 500-267
      http://www.antd.nist.gov/usgv6/docs/usgv6-v1.0.pdf
    - Include declarations of conformance per the USGv6 Testing Program
      http://www.antd.nist.gov/usgv6/testing.html
    - Be applicable according to Agency Enterprise Architectures, per OMB Memorandum 05-22
      http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf