

Table 3-1 Joint Staff IPv6 Operational Criteria

<p>Joint Staff IPv6 Operational Criteria</p>	<p>Level 1 Decomposition (Capabilities to be demonstrated)</p>	<p>Level 2 Decomposition (Specific technology/infrastructure/functionality to be demonstrated)</p>	<p>Primary Responsible DoD Component & Target Date for Final T&E Report</p>
<p>Criterion 1 Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of HAIPE, integration of IP security (IPSec), and integration with firewalls and intrusion detection systems.</p>	<p>Ensure that information is not disclosed to unauthorized persons, processes, or devices.</p>	<p>Verify implementation of IPSec with Encapsulating Security Payload (ESP) in IPv6 hosts.</p> <p>Verify the implementation of IPSec with ESP in IPv6 routers and switches.</p> <p>Verify integration with Public Key Infrastructure (PKI).</p>	<p>NSA 4QFY 2008</p>
	<p>Ensure information received is the same as that which was sent (protect against unauthorized modification or destruction of information).</p>	<p>Verify implementation of Authentication Header (AH) in IPv6 hosts.</p> <p>Verify implementation of AH in IPv6 routers and switches.</p>	<p>NSA 4QFY 2008</p>
	<p>Ensure authentication of persons and processes.</p>	<p>Verify security of Authentication, Authorization, and Accounting (AAA) servers using IPv6.</p> <p>Verify integration of AAA servers with PKI.</p>	<p>NSA 4QFY 2008</p>
	<p>Ensure availability and mitigate denial of services (timely, reliable access to data, and information services for authorized users).</p>	<p>Verify protection of the IPv6 resident protocol implementation of hosts, switches, and routers from intruders. (Note: Included in this are vulnerabilities that arise from errors in protocol specification or implementation or the associated device firmware.)</p> <p>Demonstrate IPv6 traffic filtering capabilities of routers and firewalls according to security policies.</p>	<p>NSA 4QFY 2008</p>

(Continued on next page)

Joint Staff IPv6 Operational Criteria	Level 1 Decomposition (Capabilities to be demonstrated)	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Primary Responsible DoD Component & Target Date for Final T&E Report
	Ensure IPv6 traffic is interoperable with firewalls and IDSs.	Evaluate firewalls and IDS functions that can be applied to IPv6 traffic. Evaluate firewalls and IDS functions that can be applied to tunneled IPv6 traffic.	NSA 1QFY 2008
	Ensure IPv6 traffic is interoperable with HAIPE devices.	Evaluate HAIPE v3 ability to encrypt/decrypt IPv6 packets. Evaluate HAIPE v3 ability to encrypt/decrypt tunneled IPv6 packets.	NSA 2QFY 2009
Criterion 2 Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment.	Demonstrate IPv4 application to IPv4 application over a mixed IPv4 and IPv6 network.	Demonstrate core service interoperability: Domain Name System (DNS), directory services, File Transfer Protocol (FTP), e-mail, web services, Network Time Protocol (NTP), and PKI. Demonstrate network core applications interoperability: Voice over IP (VoIP) and video over IP. Demonstrate Commercial Off The Shelf (COTS) application interoperability (transaction, database access, and web services). Demonstrate Government Off The Shelf (GOTS) applications/systems interoperability.	DISA (JITC) 2QFY 2008

(Continued on next page)

Joint Staff IPv6 Operational Criteria	Level 1 Decomposition (Capabilities to be demonstrated)	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Primary Responsible DoD Component & Target Date for Final T&E Report
	Demonstrate IPv6 application to IPv4 application over a mixed IPv4 and IPv6 network.	Demonstrate core service interoperability: DNS, Directory, FTP, e-mail, web services, NTP, and PKI. Demonstrate network core applications interoperability: VoIP and video over IP. Demonstrate COTS application interoperability (transaction, database access, and web services). Demonstrate GOTS application/system interoperability.	DISA (JITC) 2QFY 2008
	Demonstrate IPv6 application to IPv6 application over a mixed IPv4 and IPv6 network.	Demonstrate core service interoperability: DNS, Directory, FTP, e-mail, web services, NTP, and PKI. Demonstrate network core applications interoperability: VoIP and video over IP. Demonstrate COTS application interoperability (transaction, database access, and web services). Demonstrate GOTS application/system interoperability.	DISA (JITC) 2QFY 2008
(Continued on next page)			

Joint Staff IPv6 Operational Criteria	Level 1 Decomposition (Capabilities to be demonstrated)	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Primary Responsible DoD Component & Target Date for Final T&E Report
Criterion 3 Demonstrate equivalent to, or better performance than, IPv4 based networks.	Demonstrate IPv6 throughput equivalent to or better than IPv4.	Same as Level 1.	DISA (JITC) 1QFY 2008
	Demonstrate IPv6 latency equivalent to or better than IPv4.	Same as Level 1.	DISA (JITC) 1QFY 2008
	Demonstrate IPv6 packet loss equivalent to or better than IPv4.	Same as Level 1.	DISA (JITC) 1QFY 2008
	Demonstrate IPv6 service availability equivalent to or better than IPv4.	Compare service provisioning times. Compare service recovery times.	DISA (JITC) 1QFY 2008
Criterion 4 Demonstrate voice, data, and video integration.	Demonstrate simultaneous voice, data, and video (or any combination thereof) over shared IPv6 networks.	Demonstrate Quality of Service (QoS) capabilities of IPv6 networks using Differentiated Services (DiffServ) and Resource Reservation Protocol (RSVP).	NAVY 4QFY 2008
		Demonstrate transport control capabilities of IPv6 networks using Real Time Protocol (RTP).	NAVY 4QFY 2008
		Demonstrate session signaling capabilities of IPv6 networks using the Session Initiation Protocol (SIP).	NAVY 4QFY 2008
(Continued on next page)			

Joint Staff IPv6 Operational Criteria	Level 1 Decomposition (Capabilities to be demonstrated)	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Primary Responsible DoD Component & Target Date for Final T&E Report
Criterion 5 Demonstrate effective operation in low-bandwidth environment.	Same as the criterion itself.	Demonstrate ability to compress IPv6 headers using Robust Header Compression (ROHC) techniques.	ARMY 2QFY 2009
		Demonstrate ability to maintain IPv6 connectivity under low-bandwidth conditions. (Note: Point to Point Protocol will be added to demonstrate IPv6 connectivity.)	ARMY 2QFY 2009
Criterion 6 Demonstrate scalability of IPv6 networks.	Demonstrate ability to add more network resources, services, and users without negative impact on existing users.	Demonstrate ability to build IPv6 networks comparable in size to existing IPv4 networks, with equal or better performance.	DISA 1QFY 2008
		Demonstrate ability to populate IPv6 subnets with network elements in comparable numbers to existing IPv4 subnets, with equal or better performance.	DISA 1QFY 2008
		Demonstrate ability to create IPv6 multicast sessions whose sizes are comparable to existing IPv4 multicast sessions, with equal or better performance.	DISA 1QFY 2008
		Demonstrate ability to create IPv6 core services (DNS, Directory, FTP, e-mail, web services, NTP, and PKI) where the numbers of users are comparable to existing IPv4 core services, with equal or better performance.	DISA 1QFY 2008
		(Continued on next page)	

Joint Staff IPv6 Operational Criteria	Level 1 Decomposition (Capabilities to be demonstrated)	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Primary Responsible DoD Component & Target Date for Final T&E Report
Criterion 7 Demonstrate support for mobile terminals (voice, data, and video).	Demonstrate ability to maintain IPv6 applications on the move.	Demonstrate ability to maintain an existing voice, data, or video session on the move using SIP and Mobile IPv6 (MIPv6).	ARMY 2QFY 2009 *
		Demonstrate ability to initiate or accept new voice, data, or video sessions on the move using SIP and MIPv6.	ARMY 2QFY 2009 *
Criterion 8 Demonstrate transition techniques.	Demonstrate DoD-recommended network transition techniques.	Demonstrate feasibility of IPv4 and IPv6 network transition techniques: <ul style="list-style-type: none"> • Dual stack everywhere in an autonomous system • Configured tunnels • Dual Stack Transition Mechanism (DSTM) • Tunnel Broker. 	AIR FORCE 1QFY 2008
	Demonstrate DoD recommended application transition techniques.	Demonstrate the feasibility of the IPv4 and IPv6 application transition techniques: <ul style="list-style-type: none"> • Stateless IP/Internet Control Message Protocol Translation (SIIT) • Bump in the Application Program Interface (BIA) • Bump in the Stack (BIS). 	AIR FORCE 4QFY 2008
Criterion 9 Demonstrate ability to provide network management of networks.	Demonstrate ability to monitor, configure, and account for IPv6 network resources.	Demonstrate that Network Management Systems (NMS) commonly used by the DoD can monitor IPv6 devices. Demonstrate that NMS commonly used by the DoD can configure IPv6 devices. Demonstrate that IPv6 devices can be accounted by NMS commonly used by the DoD.	AIR FORCE 4QFY 2008
(Continued on next page)			

Joint Staff IPv6 Operational Criteria	Level 1 Decomposition (Capabilities to be demonstrated)	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Primary Responsible DoD Component & Target Date for Final T&E Report
Criterion 10 Demonstrate tactical deployability and ad hoc networking.	Demonstrate ability to move IPv6 networks as a whole, without reconfiguration.	Demonstrate the ability to move networks to other locations while maintaining connectivity via the original IPv6 addresses, using Network Mobility (NEMO). Demonstrate ability to move network elements to other locations while maintaining connectivity via the original IPv6 addresses, using MIPv6.	NAVY 2QFY 2010 *
	Demonstrate ability to support IPv6 networking without fixed router infrastructure.	Demonstrate ability of IPv6 hosts to forward packets from peers while on the move, using Mobile Ad hoc Networks (MANET) routing protocols.	NAVY 2QFY 2010 *

* These target dates may be adjusted to accommodate IPv6 implementation in WIN-T, JTRS, SATCOM, and other related programs of record.