Suppliers Declaration of Conformity for USGv6 Products		
1	**The Document Requiring Conformity:**	**USGv6 Profile Version 1.0, July 2008. (NIST SP500-267)**
2	**Product Identifier:**	**Red Hat Enterprise Linux**

3 Supplier's Name, Address and SDOC Contact Details

Red Hat, Inc., 100 East Davie Street, Raleigh, NC 27601, United States, contact: Jaroslav Reznik <jreznik@redhat.com>

4 Product as Tested/Declared: *Product Identifier, version/revision information, details of configuration tested.*

8.2

5 Product Family (other products using same IPv6 stack(s) to which these results are declared to apply). ***Check Product Family attestation below.***

6 USGv6 Capability summary. (For each distinct IPv6 stack in the product provide a summary of its USGv6 capabilities below and include a detailed test result summary). *e.g. example-prod-id/stack-1: USGv6-v1-Host: IPv6-Base+Addr-Arch+IPsec-v3+IKEv2+SLAC+Link=Ethernet.*

USGv6-v1-Host: IPv6-Base+Addr-Arch+SLAAC+Link = Ethernet

7 Self Contained or Composite SDOC? (Must indicate one).

YES	*All of the declared USGv6 capabilities of this product are addressed by orginal test results reported in this SDOC.*		*Some or all of the USGv6 capabilities of this product are provided by the use and/or integration of umodified components that have their own unique USGv6 SDOCs. All of the relevant referenced SDOCs are identified in section 8 and attached. This product's page 2 will indicate which capabilities are provided by specific referenced components (product-id/stack-id).*

8 Additional Declarations / Attachments: *(List supplier & product-id/stack-id for referenced and attached test results in the case of composite products).*

	Component Supplier	Product ID:	Stack ID:	Notes:
[1]				
[2]				
[3]				
[4]				

9 Supplementary Attestations *(Answer all).*

	YES	*This product is fully functional in dual stack environments.That is, no claimed capabilities are invalidated ifthis product is operated in a dual stack (6 and 4)network environment.*	YES	*This product is fully functional in IPv6 only environments. That is, no claimed capabilities are invalidated if this product is deployed in a network environment that does not support Ipv4.*
	YES	*This SDOC contains a capabilities test report for each unique IPv6 stack in the product. If not, the stacks/ports not covered are documented, and how their Ipv6 capabilities differ from those reported are explained.*	YES	*All of the products listed in the product family in section 5 are implemented such that their USGv6 capabilities are identical in form and function across the entire product family. The specific conformance and interoperability test results for the USGv6 capabilities of an identified member of this product family are provided in this SDOC. The SDOC attests that these tested USGv6 capabilitiesare identical and unmodified for all the products cited above.*

10	**Signature**		**Date**	26. 2. 2021
	Print Name / Title	Jaroslav Reznik / Program Manager		

See instructions for fields 1-12 on Page 4.

11	Suppliers Declaration of Conformity for USGv6 Products: Declared Capabilities and Test Results Summary								
Product Id:	**Red Hat Enterprise Linux**		**Stack Id:**			**8.2**			
Spec /			Context /	**Supported Capabilities**			**USGv6 Testing Program Results**			
Reference	Section	**USGv6-v1 Profile Requirements**	Configuration	**Host**	**Router**	**NPD**	Test Suite	Test Lab / Result ID, Note #, or	Test Suite Interoperability	Test Lab / Result ID, Note #, or
SP500-267	**6.1**	**IPv6 Basic Requirements**								
		support of IPv6 base (IPv6;ICMPv6;PMTU;ND)	IPv6-Base	P			**Basic_v1.*_C**	UNH-IOL/32132	**Basic_V1.*_I**	UNH-IOL/32133
		support of PMTU Discovery Protocol requirements	PMTU	P			**Basic_v1.*_C**	UNH-IOL/32132	**Basic_V1.*_I**	UNH-IOL/32133
		support of stateless address auto-configuration	SLAAC	P			**SLAAC-V1.*_C**	UNH-IOL/32132	**SLAAC-V1.*_I**	UNH-IOL/32133
		support of Creation of Global Addresses	SLAAC - c(M)	P			**SLAAC-V1.*_C**	UNH-IOL/32132	**SLAAC-V1.*_I**	UNH-IOL/32133
		support of SLAAC privacy extensions.	PrivAddr				*Self Test*		*Self Test*	
		support of stateful (DHCP) address auto-	DHCP-Client				**DHCP_Client_v1.*_C**		**DHCP_Client_v1.*_I**	
		support of automated router prefix delegation	DHCP-Prefix				*Self Test*		*Self Test*	
		support of neighbor discovery security extensions	SEND							
SP500-267	**6.6**	**Addressing Requirements**								
		support of addressing architecture reqts	Addr-Arch	P			**Addr_Arch_v1.*_C**	UNH-IOL/32134	**Addr_Arch_v1.*_I**	UNH-IOL/32136
		support of cryptographically generated addresses	CGA							
SP500-267	**6.7**	**IP Security Requirements**								
		support of the IP security architecture	IPsecv3	N			**IPsecv3_v1.*_C**	UNH-IOL/32206	**IPsecv3_v1.*_I**	UNH-IOL/32207, Note 1, 2
		support for automated key management	IKEv2	N			**IKEv2_v1.*_C**	UNH-IOL/32208, Note 3	**IKEv2_v2.*_I**	UNH-IOL/32209, Note 3
		support for encapsulating security payloads in IP	ESP	N			**ESPv3_v1.*_C**	UNH-IOL/32206	**ESP_v1.*_I**	UNH-IOL/32207, Note 1, 2
SP500-267	**6.11**	**Application Requirements**								
		support of DNS client/resolver functions	DNS-Client				*Self Test*		*Self Test*	
		support of Socket application program interfaces	SOCK				*Self Test*		*Self Test*	
		support of IPv6 uniform resource identifiers	URI							
		support of a DNS server application	DNS-Server				*Self Test*		*Self Test*	
		support of a DHCP server application	DHCP-Server				*Self Test*		**DHCP_Serv_v1.*_I**	
SP500-267	**6.2**	**Routing Protocol Requirements**								
		support of the intra-domain (interior) routing protocols	IGW				*Self Test*		**OSPFv3_v1.*_I**	
		support for inter-domain (exterior) routing protocols	EGW				*Self Test*		**BGP_v1.*_I**	
SP500-267	**6.4**	**Transition Mechanism Requirements**								
		support of interoperation with IPv4-only systems	IPv4				*Self Test*		*Self Test*	
		support of tunneling IPv6 over IPv4 MPLS services	6PE				*Self Test*		*Self Test*	
SP500-267	**6.8**	**Network Management Requirements**							Self Test	
		support of network management services	SNMP				*Self Test*		Self Test	
SP500-267	**6.9**	**Multicast Requirements**								
		support of basic multicast	Mcast				*Self Test*			
		full support of multicast communications	SSM				*Self Test*		*Self Test*	
SP500-267	**6.10**	**Mobility Requirements**								
		support of mobile IP capability.	MIP				*Self Test*		*Self Test*	
		support of mobile network capabilities	NEMO				*Self Test*		*Self Test*	
SP500-267	**6.3**	**Quality of Service Requirements**								
		support of Differentiated Services capabilities	DS				*Self Test*		*Self Test*	
SP500-267	**6.12**	**Network Protection Device Requirements**								
		support of common NPD reqts	NPD				**N1|N2|N3|N4_v1.3**			
		support of basic firewall capabilities	FW				**N1_FW_v1.3**			
		support of application firewall capabilities	APFW				*Self Test*			
		support of intrusion detection capabilities	IDS				**N3_IDS_v1.3**			
		support of intrusion protection capabilities	IPS				**N4_IPS_v1.3**			
SP500-267	**6.5**	**Link Specific Technologies**								
		support of robust packet compression services	ROHC				Self Test		Self Test	
		support of link technology [O:1]	Link=Ethernet	P			Self Test	*Self Declaration*	Self Test	*Self Declaration*
		(repeat as needed) support of link technology	Link=							
12		**< Check HERE if this stack's DOC includes additional information about tested capabilities and options on an attached page 3 of notes.**								

Level	**Level of support for USGv6-v1 Requirements for capability.**	**Color**	**Indication of USGv6-v1 Recommended Level of Support for device type / stack role.**
	Blank - SDOC makes no declaration for this capability.		Indicates capability that is recommendend as mandatory (unconditional MUST) in the USGv6-v1 Profile.
P	Passed required tests of USGv6-V1 requirements for these capabilities.		Indicates cabability that is unusal for a given device type / stack role. Do not select without careful analysis.
N	See notes page for details on the level of support of USGv6-v1 reequirements for this capability.		Indicates capability that is left optional / ocnditional by the recommedations of the USGv6-v1 Profile.
X	USGv6 capability not supported in product.		

Test Suite - Specific USGv6 Test suite used for test. See: http://www.antd.nist.gov/usgv6/test-specifications.html

Test Lab / Result ID - Abbreviation of accredited laboratory and its local identifier for this test result.

Note # - reference to a detailed note about this capability or result on attached page.

Component Ref - Supplier / Product / Stack ID of distinctly tested component that provides this capability.

Field 13	Product Id:		Red Hat Enterprise Linux		Stack Id:			8.2			
					Supported Capabilities			Notes about USGv6-v1 Capabilities.			
Note #	Spec / Reference	Section	USGv6-v1 Profile Requirements	Context / Configuration	Host	Router	NPD	Test Suite	Test Lab / Result ID, Note	Test Suite	Test Lab / Result ID, Note
1	RFC4301		**Security Architecture for the IP**	IPsec-v3	**M**					IPsecv3_v1.*_I	UNH-IOL/32207, Note 1
Discussion:	After receiving a valid unencrypted Packet Too Big message the DUT did not transmit an Echo Response packet.										
2	RFC4303		**Encapsulating Security Payload (ESP)**	IPsec-v3	**M**					IPsecv3_v1.*_I	UNH-IOL/32207, Note 2
Discussion:	The DUT did not transmit a tunneled, fragmented Echo Request packet.										
3	RFC5114		**Diffie-Hellman MODP group 24**	IKEv2	**M**			IKEv2_v1.*_C	UNH-IOL/32208, Note 3	IKEv2_v2.*_I	UNH-IOL/32209, Note 3
Discussion:	The device under test does not support Diffie-Hellman group 24.										
4											
Discussion:											
5											
Discussion:											
6											
Discussion:											
7											
Discussion:											
8											
Discussion:											
9											
Discussion:											
10											
Discussion:											

Vendor's General Notes / Discussion about this Product / Stack's capabilities:

	Spec / Reference	Section	USGv6-v1 Requirements Title / Definition	Context / Configuration	USGv6-V1 Rec Host	Router	NPD	Notes about requested USGv6-v1 Capabilities.			
			IPv6 Basic Requirements								
	RFC2460		**IPv6 Specification**	IPv6-Base	**M**	**M**					
		2	IPv6 Packets: send, receive	IPv6-Base	**M**	**M**					
		2	IPv6 packet forwarding	IPv6-Base		**M**					

		4	Extension headers: processing	IPv6-Base	**M**	**M**					
		4.3	Hop-by-Hop & unrecognized options	IPv6-Base	**M**	**M**					
		4.5	Fragment headers: send, receive, process	IPv6-Base	**M**	**M**					
		4.6	Destination Options extensions	IPv6-Base	**M**	**M**					
	RFC5095		**Deprecation of Type 0 Routing Headers**	IPv6-Base	**M**	**M**					
	RFC2711		**IPv6 Router Alert Option**	IPv6-Base		**M**					
	RFC4443		**ICMPv6**	IPv6-Base	**M**	**M**					
	RFC4884		**Extended ICMP for Multi-Part Messages**		S+	S+					
	RFC1981		**Path MTU Discovery for IPv6**	IPv6-Base	**M**	**M**					
		4	Discovery Protocol Requirements	IPv6-Base	**M**	S+					
	RFC2675		**IPv6 Jumbograms**		O	O					
	RFC4861		**Neighbor Discovery for IPv6**	IPv6-Base	**M**	**M**					
		4.1, 4.2	Router Discovery	IPv6-Base	**M**	**M**					
		4.6.2	Prefix Discovery	IPv6-Base	**M**	**M**					
		7.2	Address Resolution	IPv6-Base	**M**	**M**					
		7.2.5	NA and NS processing	IPv6-Base	**M**	**M**					
	(RFC4862)	7.2.3	Duplicate Address Detection	IPv6-Base	**M**	**M**					
		7.3	Neighbor Unreachability Detection	IPv6-Base	**M**	**M**					
		8	Redirect functionality		S	**M**					
	RFC5175		**IPv6 Router Advertisement Flags Option**		S	S					
	RFC4191		**Default Router Preference**		S+	S+					
	RFC3971		**Secure Neighbor Discovery**	SEND	c(M)	c(M)					
			Auto Configuration								
	RFC4862		**IPv6 Stateless Address Autoconfig**	SLAAC	c(M)						
		5.3	Creation of Link Local Addresses	SLAAC	**M**	**M**					
	(RFC4861)	5.4	Duplicate Address Detection	SLAAC	**M**	**M**					
		5.5	Creation of Global Addresses	SLAAC	c(M)						
		*	Ability to Disable Creation of Global Addrs	SLAAC	c(M)						
	RFC4941		**Privacy Extensions for IPv6 SLAAC**	SLAAC & PriAddr	c(M)						
		*	<2nd context for MIP Mobile Node>	SLAAC & MIP	c(S+)						
	RFC3736		**Stateless DHCP Service for IPv6**	SLAAC	c(S+)						
	RFC3315		**Dynamic Host Config Protocol (DHCPv6)**	DHCP-Client	c(M)						
		*	Ability to Administratively Disable	DHCP-Client	c(M)						
			DHCP Client Functions	DHCP-Client	c(M)						
	RFC4361		**Node-specific Client IDs for DHCPv4**	DHCP-Client	c(S+)						
	RFC3633		**Prefix Delegation**	DHCP-Prefix		c(M,S+)					
			Addressing Requirements								
	RFC4291		**IPv6 Addressing Architecture**	Addr-Arch	**M**	**M**					
	RFC4007		IPv6 Scoped Address Architecture	Addr-Arch	**M**	**M**					
		*	Ability to manually configure Addresses	Addr-Arch	**M**	**M**					
	RFC4193		Unique Local IPv6 Unicast Address		O	O					
	RFC3879		Deprecating Site Local Addresses	Addr-Arch	**M**	**M**					
	RFC3484		Default Address Selection for IPv6	Addr-Arch	**M**	**M**					
		2.1	Configurable Selection Policies		S+	S+					
	RFC2526		Reserved IPv6 Subnet Anycast Addresses	Addr-Arch	**M**	**M**					
	RFC3972		**Cryptographically Generated Addresses**	SEND or CGA	c(M)	c(M)					
	RFC4581		(CGA) Extension Field Format	SEND or CGA	c(M)	c(M)					
	RFC4982		(CGA) Support for Multiple Hash Algos.	SEND or CGA	c(M)	c(M)					
			Application Requirements								
	RFC3596		**DNS Extensions for IPv6**	DNS-Client	c(M)	c(M)					
		2.1	Support of AAAA records	DNS-Client	c(M)	c(M)					
		2.5	Support of ipv6.arpa PTR records	DNS-Client	c(M)	c(M)					
	RFC2671		**Extension Mechanisms for DNS (EDNS0)**	DNS-Client	c(M)	c(M)					
	RFC3226		**DNSSEC and IPv6 DNS MSG Size Reqs**	DNS-Client	c(M)	c(M)					
	RFC3986		**URI: Generic Syntax**	URI	c(M)	c(M)					
	RFC3493		**Basic Socket API for IPv6**	SOCK	c(M)						
	RFC3542		Advanced Socket API for IPv6	SOCK & MIP	c(M)						
	RFC4584		Extension to Sockets API for Mobile IPv6	SOCK & MIP	c(M)						
	RFC3678		Socket API Extensions Multicast Source Filters	SOCK & SSM	c(M)						
	RFC5014		Socket API for Source Address Selection	SOCK	c(S+)						
			Specific Applications								
	RFC3596		DNS Server Functions	DNS-Server	c(M)	c(M)					
	RFC3315		DHCPv6 Server Functions	DHCP-Server	c(M)	c(M)					
			Routing Protocol Requirements								
			Interior Routing Protocol								
	RFC2740		**OSPF for IPv6**	IGW		c(M)					
	RFC4552		Authentication/Confidentiality for OSPFv3	IGW		c(M)					

			Exterior Routing Protocol									
	RFC4271		**Border Gateway Protocol 4 (BGP-4)**	EGW or 6PE		c(M)						
	RFC1772		BGP Application in the Internet	EGW or 6PE		c(M)						
	RFC4760		BGP Multi-Protocol Extensions	EGW or 6PE		c(M)						
	RFC2545		BGP Multi-Protocol Extensions for IPv6 IDR	EGW or 6PE		c(M)						
			IP Security Requirements									
			IPsec-v3									
	RFC4301		**Security Architecture for the IP**		**M**	**M**						
		4.1	Support of Transport Mode SAs	IGW or IPv4	**M**	c(M)						
		4.5.1	Manual SA and Key Management		**M**	**M**						
		4.5.2	Automated SA and Key Management		**M**	**M**						
	RFC4303		Encapsulating Security Payload (ESP)	IPsec-v3	**M**	**M**						
	RFC4302		Authentication Header (AH)	IPsec-v3	O	O						
	RFC3948		UDP Encapsulation of ESP Packets	IPsec-v3	O	O						
	RFC4835		Cryptographic Algorithms for ESP and AH	IPsec-v3	**M**	**M**						
		*	(See additional 4835 requirements below)									
	RFC4308		Cryptographic Suites for IPsec	IPsec-v3	O	O						
		2.1	VPN-A	IPsec-v3	S	S						
		2.2	VPN-B	IPsec-v3	S+	S+						
	RFC4869		Suite B Cryptographic Suites for IPsec	IPsec-v3	O	O						
	RFC4809		Requirements for an IPsec Cert Mgmnt Profile	IPsec-v3	S+	S+						
			IKEv2									
	RFC4306		**Internet Key Exchange (IKEv2) Protocol**	IKEv2	**M**	**M**						
		4	Pre-shared secrets for peer authentication	IKEv2	**M**	**M**						
		4	RSA sig auth	IKEv2	**M**	**M**						
		4	NAT-T in IKEv2	IKEv2	O	O						
		3.3.3	ESN	IKEv2	**M**	**M**						
	RFC4718		IKEv2 Clarifications & Impl. Guidelines	IKEv2	S	S						
	RFC4307		Cryptographic Algorithms for IKEv2	IKEv2	**M**	**M**						
			(See additional 4307 requirements below)									
	RFC3526		More MODP DH Groups for IKE	IKEv2	S	S						
	RFC5114		Additional DH Groups for Use with IETF Stds	IKEv2	O	O						
		2.3,3.2	Diffie-Hellman MODP group 24	IKEv2	**M**	**M**						
	RFC4945		Internet IPsec PKI Profile of IKEv1, IKEv2 & PKIX	IKEv2	S+	S+						
			Uses of Cryptographic Algorithms									
	RFC2410		NULL Encryption		**M**	**M**						
	RFC4835	3.1.1	NULL Encryption	ESP	**M**	**M**						
	RFC2451		ESP CBC-mode Algorithms		**M**	**M**						
		2.6	3DES-CBC	ESP	**M**	**M**						
	RFC4835	3.1.1	3DES-CBC	ESP	**M**	**M**						
	RFC4307	3.1.1	3DES-CBC	IKEv2	**M**	**M**						
	RFC3602		AES-CBC		**M**	**M**						
	RFC4835	3.1.1	AES-CBC with 128 bit keys	ESP	**M**	**M**						
	RFC4307	3.1.1	AES-CBC with 128 bit keys	IKEv2	**M**	**M**						
	RFC3686		AES-CTR		S	S						
	RFC4835	3.1.1	AES-CTR with 128-bit keys	ESP	S	S						
	RFC4307	3.1.3	AES-CTR with 128-bit keys	IKEv2	S	S						
	RFC4309		AES-CCM		O	O						
	RFC4835	3.1.2	AES-CCM with 128 bit keys	ESP	O	O						
	RFC4106		AES-GCM		O	O						
		6	128-bit ICV	ESP	O	O						
		8.1	AES-GCM with 128 bit keys	ESP	O	O						
	RFC4543		AES-GMAC		O	O						
		5.4	ENCR-NULL-AUTH-AES-GMAC 128 bit keys	ESP	O	O						
		5.4	AUTH-AES-GMAC with 128 bit keys	AH	O	O						
	RFC2404		HMAC-SHA-1-96		**M**	**M**						
	RFC4835	3.1.1/3.2	HMAC-SHA-1	ESP or AH	**M**	**M**						
	RFC4307	3.1.1	HMAC-SHA-1	IKEv2	**M**	**M**						
	RFC4307	3.1.4	HMAC-SHA-1 as a PRF	IKEv2	**M**	**M**						
	RFC4868		HMAC-SHA-256		S+	S+						
		2.3	HMAC-SHA-256-128	ESP or AH	S+	S+						
		2.3	HMAC-SHA-256-128	IKEv2	S+	S+						
		2.4	HMAC-SHA-256 as a PRF	IKEv2	S+	S+						
	RFC3566		AES-XCBC-MAC-96		S+	S+						
	RFC4835	3.1.1/3.2	AES-XCBC-MAC-96	ESP or AH	S+	S+						
	RFC4307	3.1.5	AES-XCBC-MAC-96	IKEv2	S+	S+						
	RFC4434		AES-XCBC-PRF-128		S+	S+						
	RFC4307	3.1.4	AES128-XCBC-PRF	IKEv2	S+	S+						
			Transition Mechanisms Requirements									

	RFC4038		**Application Aspects of IPv6 Transition**	IPv4	S						
	RFC4213		**Transition Mech. for Hosts & Routers**	IPv4	c(M)	c(M)					
		2	Dual Stack IPv4 and IPv6	IPv4	c(M)	c(M)					
		3	Configured Tunnels	IPv4	c(S)	c(M)					
	RFC4891		Using IPsec to Secure IPv6-in-IPv4 Tunnels	IPv4	c(S)	c(M)					
	RFC2473		Generic Packet Tunneling in IPv6	IPv4		c(M)					
	RFC2784		Generic Routing Encapsulation	IPv4		c(S+)					
			IPv6 Provider Edge MPLS Tunneling								
	RFC4798		Connecting IPv6 islands over IPv4 MPLS (6PE)	IPv4 & 6PE		c(M)					
			Network Management Requirements								
	RFC3411		**SNMP v3 Management Framework**	SNMP	c(M)	**M**					
	RFC3412		SNMP Message Process and Dispatch	SNMP	c(M)	**M**					
	RFC3413		SNMP Applications	SNMP	c(M)	**M**					
		1.2	Command Responder	SNMP	c(M)	**M**					
		1.3	Notification Generator	SNMP	c(S)	**M**					
	RFC3414		User-based Security Model for SNMPv3	SNMP	c(M)	**M**					
			Management Information Bases								
	RFC4293		MIB for the IP	SNMP	c(M)	**M**					
	RFC4292		MIB for IP Forwarding Table	SNMP		**M**					
	RFC4022		MIB for TCP	SNMP	c(S+)	S+					
	RFC4113		MIB for UDP	SNMP	c(S+)	S+					
	RFC4087		MIB for IP Tunnels	SNMP & IPv4		c(M)					
	RFC4807		MIB for IPsec Policy Database Configuration	SNMP & IPsec-v3		**M**					
	RFC4295		MIB for Mobile IP	SNMP & MIP		c(M)					
	RFC3289		MIB for DiffServ	SNMP & DS		**M**					
			Multicast Requirements								
	RFC3810		**MLD Version 2 for IPv6**	Mcast	**M**	**M**					
	RFC3306		**Unicast-Prefix-based IPv6 Mcast Addresses**	Mcast	**M**	**M**					
	RFC3307		**Allocation Guidelines for IPv6 Mcast Addrs**	Mcast	**M**	**M**					
	RFC4607		**Source-Specific Multicast for IP**	SSM	c(M)	c(M)					
	RFC4604		MLDv2 for Source Specific Multicast (SSM)	SSM	c(M)	c(M)					
			Protocol Independent Multicast (PIM)								
	RFC4601		PIM Sparse Mode (SM)	SSM		c(S+)					
	RFC4609		PIM-SM Security Issues / Enhancements	SSM		c(S)					
	RFC3956		Embedding Rendezvous Point (RP) Mcast Addr	SSM		c(S+)					
			Mobility Requirements								
	RFC3775		**Mobility Support in IPv6**	MIP	c(M)	c(M)					
		8.1	All Nodes as Correspondent Node	MIP	**M**						
		8.2	Route Optimization	MIP	c(M)						
		8.2	Allow route optimization to be disabled.	MIP	c(M)						
		8.3	All IPv6 Routers	MIP		**M**					
		8.4	Home Agents	MIP		c(M)					
		8.5	Mobile Nodes	MIP	c(M)						
	RFC4282		The Network Access Identifier	MIP	c(S+)	c(S+)					
	RFC4283		Mobile Node Identifier option for MIPV6	MIP	c(S+)	c(S+)					
	RFC4877		MIPv6 Op with IKEv2 and Revised IPsec Arch	MIP	c(M)	c(M)					
	RFC3963		Network Mobility (NEMO) Basic Support	NEMO		c(M)					
			Quality of Service Requirements								
	RFC2474		**Differentiated Services (DiffServ)**	DS	c(M)	**M**					
	RFC2475		An Architecture for Differentiated Services	DS		S					
	RFC3260		New Terminology / Clarifications for Diffserv	DS		S					
	RFC2983		Differentiated Services and Tunnels	DS		S					
	RFC4594		Config Guidelines for DS Service Classes	DS		S					
	RFC3086		Def. of DiffServe Per Domain Behaviors (PDB)	DS		S					
	RFC3140		Per Hop Behavior (PHB) Identification Codes	DS	c(M)	**M**					
	RFC2597		Assured Forwarding PHB Group	DS		S+					
	RFC3246		An Expedited Forwarding PHB	DS		S+					
	RFC3247		Supplemental Info for the New EF PHB	DS		S+					
	RFC3168		**Explicit Congestion Notification (ECN) to IP**	ECN	S	S+					
			Link Specific Requirements								
	RFC2464		IPv6 over Ethernet	Link	c(M)	c(M)					
	RFC2467		IPv6 over FDDI	Link	c(M)	c(M)					
	RFC5072		IPv6 over PPP	Link	c(M)	c(M)					
	RFC2491		IPv6 over Non-Broadcast Multiple Access (NBMA) net	Link	c(M)	c(M)					
	RFC2492		IPv6 over ATM Networks	Link	c(M)	c(M)					
	RFC2497		IPv6 over ARCnet	Link	c(M)	c(M)					
	RFC2590		IPv6 over Frame Relay	Link	c(M)	c(M)					
	RFC3146		IPv6 over IEEE 1394 Networks	Link	c(M)	c(M)					
	RFC3572		IPv6 over MAPOS (SONET/SDH)	Link	c(M)	c(M)					
	RFC4338		IPv6 & IPv4 over Fibre Channel	Link	c(M)	c(M)					
	RFC4944		IPv6 over IEEE 802.15.4 Networks	Link	c(M)	c(M)					
			Packet Compression Technologies								

	RFC2507		IP Header Compression		O	O					
	RFC3173		IP Payload Compression Protocol (IPComp)		O	O					
	RFC4995		RObust Header Compression (ROHC) Framework	ROHC	c(M)	c(M)					
	RFC4996		ROHC Profile for TCP	ROHC	c(M)	c(M)					
	RFC3095		ROHC Profiles for RTP, UDP, ESP and Uncomp	ROHC	c(M)	c(M)					
	RFC4815		Corrections and Clarifications to RFC3095	ROHC	c(M)	c(M)					
	RFC3843		ROHC Profile for IP Only	ROHC	c(S+)	c(S+)					
	RFC3241		ROHC over PPP	ROHC & Link	c(M)	c(M)					
	RFC4362		ROHC: Link Assisted for IP/UDP/RTP	ROHC	c(S+)	c(S+)					
			Network Protection Device Requirements								
	SP500-267	6.12.3.1	IPv6 connectivity	NPD			**M**				
	SP500-267	6.12.3.2	Dual Stack	NPD			**M**				
	SP500-267	6.12.3.3	Administrative Functionality	NPD			**M**				
	SP500-267	6.12.3.4	Authentication and Authorization	NPD			**M**				
	SP500-267	6.12.3.5	Security of Control and Comms	NPD			**M**				
	SP500-267	6.12.3.6	Persistence	NPD			**M**				
	SP500-267	6.12.3.7	Logging and Alerts	NPD			**M**				
	SP500-267	6.12.3.8	Fragmented Packets Handling	NPD			**M**				
	SP500-267	6.12.3.9	Tunneled Traffic Handling	NPD			**M**				
	SP500-267	6.12.4.1.1	Port/protocol/address blocking	FW or APFW			c(M)				
	SP500-267	6.12.4.1.2	Asymmetrical Blocking	FW or APFW			c(M)				
	SP500-267	6.12.4.1.3	IPsec Traffic Handling	FW or APFW			c(M)				
	SP500-267	6.12.4.1.4	Performance Under Load, Fail Safe	FW or APFW			c(M)				
	SP500-267	6.12.4.2.1	No violation of trust barriers	APFW			c(M)				
	SP500-267	6.12.4.2.2	Session Traffic Auth	APFW			c(M)				
	SP500-267	6.12.4.2.3	Email, File Filtering	APFW			c(M)				
	SP500-267	6.12.5.1.1	Known Attack Detection	IDS or IPS			c(M)				
	SP500-267	6.12.5.1.2	Malformed pkt detection	IDS or IPS			c(M)				
	SP500-267	6.12.5.1.3	Port scan detection	IDS or IPS			c(M)				
	SP500-267	6.12.5.1.4	Tunneled traffic detection	IDS or IPS			c(M)				
	SP500-267	6.12.5.1.5	Logging and Alerts	IDS or IPS			c(M)				
	SP500-267	6.12.5.1.6	Performance Under Load, Fail Safe	IDS or IPS			c(M)				
	SP500-267	6.12.5.2.1	Intrusion Prevention	IPS			c(M)				

General: This document describes network product from the identified supplier that claims support of USGv6 capabilities. General product and supplier identification is given on Page 1. Overall results of testing USGv6 capabilities for conformance, interoperability and network protection are given on Page 2. Detailed instructions for completing and interpreting each numbered field are given below. Note USGv6 Testing website at: http://www.antd.nist.gov/usgv6/testing.html. Contact: usgv6-project@antd.nist.gov.

Field	Description and Instructions
1	**The Document Requiring Conformity**: Identifies the profile version implemented. Not a user completable field.
2	**Product Identifier**: Supplier's concise name for the product declared.
3	**Suppliers Name, Address and Contact Details**: Company name and point of contact for SDOC questions, street address, phone and email.
4	**Product as Tested/Declared**: Product Identifier and detailed version information. If this SDOC reports oringal test results (page 2), include information about the specific product configuration(s) that was actually tested (e.g., hardware configuration, operating system, etc).
5	**Product Family**: A list of other products that use the same, unmodified IPv6 stacks such that their USGv6 capabilities are identical in form and function to the specific product configuration above. Test labs are only required to affirm the results for specific products tested. Test labs optionally may affirm recognized product families.
6	**USGv6 Capability Summary**: The USGv6 stack implementation summary as identified by the '+' notation described in the USGv6 profile, Appendix A. For each IPv6 stack implementation in the product, a distinct Stack Id and reference to the attached Results Summary page (Page 2).
7	**Self Contained or Composite SDOC**: If this SDOC relies on the test results of other disinct products, list the Supplier & Product ID/Stack IDs referenced and attach those original SDOCs to this one.
8	**Additional Declarations / Attachements:** List the supplier / product ID / Stack ID of any test results of composite components referenced by this SDOC.
9	**Supplementary Attestations**: Suppliers disclosure of IPv6 only capabilities; multiple stacks present; product family applicabilities. These are not included to qualify or disqualify a product from purchase considerations, but to inform network administrators of potential configuration options relevant to USGv6 interoperability. Check all that apply.
10	**Signature Block**: Wet ink signature of the responsible product manager, dated. Printed name and position title on the line below.

Field	Description and Instructions
11	**Summary of Results**: The format of this table mirrors the USGv6-v1.0 capabilities checklist (USGv6 Profile, Appendix A). The 12 categories of USGv6 capabilities are listed as subheadings, with subsidiary functions as line items. Configuration options related to conditional implementation of selected capabilities. **Product Id/Stack Id**: The identification line of this page includes space for Product Id and Stack Id labels. Product Id is the same as given on Page 1. As there may be more than one unique IPv6 stack implemented in the product, the Stack Id field identifies the particular stack described. One Results Summary page per stack is required. **Host, Router and Network Protection (NPD)** columns identify 'preferred' options: cells in green represent the NIST recommendations. Cells in grey denote atypical options, very unlikely to be implemented. The procuring Agency may additionally tailor these fields to indicate requirements for this acquisition. **Test Suite Conformance and Interoperability** columns identify capability sets for which a public test suite exists, and the versions applicable to USGv6-v1.0 test results. Major version v1 and all its minor versions are deemed acceptable. Over time, new versions will be added and older ones retired. There may be periods when more than one major version is acceptable concurrently. The supplier completes the adjacent Test Lab and Result Id column with the test lab acronym and unique result identifier (See Test Lab and Accreditor page on the Website). The buyer may opt to query results with the test laboratory using the specified Result Id(s). The supplier may opt to provide particular explanation of some results (partial results, additional options) in which case reference to note on an attached page 3. (e.g. "See Note# N"). See the USGv6 testing website to identify the test lab, and find contact details. Cells marked ***Self Test*** have no associated public test suite. If implemented by the supplier, the required adjacent annotation is "*Self Declaration*". Note that vendors declaring support for such a capability are declaring support for the associated specific requirements in the USGv6 Profile.
12	**Additional Options Tested**: Vendor checks if it is desired to record tested options not part of the 'Musts' in the profile. Explanations on the page following the results summary. **Headings and Special Notations**: as described. **Options for Test Lab and Result Id:** Currently 3 cases: (1) the test lab acronym and alphanumeric Id of the result set as assigned by the test laboratory; (2) 'Self declaration' denoting the supplier attests to adequate QA testing of the capability; (3) See attachment or note 'N', where the supplier explains variations in greater detail.
13	**Stack-1 Notes Instructions**: The supplier may choose to use the Notes (page 3) in order to clarify unsupported features or non passing results. Each Note # must reference the same Note # from Page 2. Complete the Note by including the Spec/Reference and Section (i.e. RFC or USGv6 Profile version), USGv6-v1 Profile Requirements, Config Option (i.e. IPv6-Base), choosing Host/Router/NPD, and Test Selection table version along with Test Lab Result ID. The Discussion includes details about the test result that will be disclosed to the buyer.

Further Description: http://www.antd.nist.gov/usgv6/testing.html, and NIST SP 500-267 USGv6 Testing Program Users Guide available at the website.