

To whom it may concern:

Please allow this letter and attached exhibit to serve as a formal response by StillSecure regarding our compliance with DoD IPv6 support requirements.

Very truly yours,

James Brown
VP of Engineering
StillSecure

EXHIBIT “A”

The table below is based on USGIPv6-V1.0 (<http://www.antd.nist.gov/usgv6-v1-draft.pdf>). StillSecure has highlighted all mandated requirements and responded with whether StillSecure Safe Access and VAM will meet these requirements. Items not applicable have been marked with a N/A.

Group	Specification / Condition	Section	Title / Definition	Condition/ Context	USGIPv6-V1.0	
					Host	NPD
					Safe Access Management Server / VAM Central Server	Safe Access Enforcement Server / VAM Distributed Server
Basic			IPv6 Basic Protocol Functionality			
	RFC2460		IPv6 Specification		☑	☑
		2	IPv6 Packets: send, receive		☑	☑
		2	IPv6 packet forwarding		NA	☑
		4	Extension headers: processing		☑	☑
		4.3	Hop-by-Hop & unrecognized options		☑	☑
		4.5	Fragment headers: send, receive, process		☑	☑
		4.6	Destination Options extensions		☑	☑
	RFC1981		Path MTU Discovery M&S		☑	☑

	RFC4443		ICMPv6		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC2461		Neighbor Discovery for IPv6		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		4.1, 4.2	Router Discovery		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		4.6.2	Prefix Discovery		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		7.2	Address Resolution		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		7.2.5	NA and NS processing		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	(RFC2462)	7.2.3	Duplicate Address Detection		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		7.3	Neighbour Unreachability Detection		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		8	Redirect Functionality		N/A	<input checked="" type="checkbox"/>
	RFC2462		IPv6 Stateless Address Autoconfig		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		5.3	Creation of Link Local Addresses		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	(RFC2461)	5.4	Duplicate Address Detection		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		5.5	Creation of Global Addresses		<input checked="" type="checkbox"/>	N/A
			Manual Address Config & Ability to Administratively Disable 2462 Creation of Global Addresses		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC3736		Stateless DHCP Service for IPv6		<input checked="" type="checkbox"/> Management Server is a static address	N/A
	RFC3315		Dynamic Host Config Protocol (DHCPv6)		<input checked="" type="checkbox"/> Management is a Static address	N/A
			Ability to Administratively Disable	DHCP	<input checked="" type="checkbox"/>	N/A
Address			Addressing Requirements			

	RFC4291		IPv6 Addressing Architecture		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4007		IPv6 Scoped Address Architecture		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4193		Unique Local IPv6 Unicast Address		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC3879		Deprecating Site Local Addresses		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
			Mobile Hosts on Open public networks	MIP	<input checked="" type="checkbox"/>	N/A
	RFC3484		Default Address Selection for IPv6		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Apps			Application Environment			
	RFC3986		URI: Generic Syntax		<input checked="" type="checkbox"/>	N/A
	RFC3596		DNS Extensions for IPv6	DNS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		2.1	Support of AAAA records	DNS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		2.5	Support of ipv6.arpa PTR records	DNS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC2671		Extension Mechanisms for DNS (EDNS0)	DNS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC3493		Basic Socket API for IPv6	SOCK	<input checked="" type="checkbox"/>	N/A
IPsec			Security Subprofile			
			IPsec-v2			
	RFC2401		Security Architecture for the Internet Protocol		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC2406		ESP	IPsec-v2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

		5	Null Authentication	IPsec-v2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
			IPsec-v3			
	RFC4303		ESP	IPsec-v3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
			IKEv1			
	RFC2409		IKEv1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC2407		The Internet IP Security DOI for ISAKMP	IKEv1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC2408		ISAKMP	IKEv1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4109		Algorithms for IKEv1	IKEv1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		3	Pre-shared secrets	IKEv1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		3	Diffie-Hellman MODP group 2	IKEv1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4304		ESN Addendum to IPsec DOI for ISAKMP	IKEv1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
			IKEv2			
	RFC4306		IKEv2		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		4	Pre-shared secrets	IKEv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		4	RSA sig auth	IKEv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		4	NAT-T in IKEv2	IKEv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		3.3.3	ESN	IKEv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4307		Cryptographic Algorithms for IKEv2	IKEv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		3.1.2	Diffie-Hellman MODP group 2	IKEv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

			Uses of Cryptographic Algorithms			
	RFC2410	18	NULL Encryption		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4305	3.1.1	NULL Encryption	ESP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC2451		ESP CBC-mode Algorithms			
		2.6	3DES-CBC	ESP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4305	3.1.1	3DES-CBC	ESP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4109	3	3DES-CBC	IKEv1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4307	3.1.1	3DES-CBC	IKEv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC3602		AES-CBC			
	RFC4305	3.1.1	AES-CBC with 128 bit keys	ESP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4109	3	AES-CBC with 128 bit keys	IKEv1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC4307	3.1.1	AES-CBC with 128 bit keys	IKEv2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Transition			IPv6 Transition Mechanisms Subprofile			
	RFC4213		Transition Mechanisms for IPv6 Hosts and Routers			
		2	Dual Stack IPv4 and IPv6		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Net Mgmt			Network Management Subprofile			
	RFC3411		SNMP v3 Management Framework			
	RFC3412		SNMP Message Process and Dispatch		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

	RFC3413		SNMP Applications		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		1.2	Command Responder		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		1.3	Notification Generator		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RFC3414		User-based Security Model for SNMPv3		<input checked="" type="checkbox"/>	N/A
	RFC4293		MIB for the IP		<input checked="" type="checkbox"/>	N/A
Link			Link Specific Technologies			
	RFC2464		IPv6 over Ethernet	Link	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NPD			Network Protection Subprofile			
	SP500-26	3.11.2.1	IPv6 connectivity	NPD	N/A	<input checked="" type="checkbox"/>
	SP500-26	3.11.2.2	Dual Stack	NPD	N/A	<input checked="" type="checkbox"/>
	SP500-26	3.11.2.3	Administrative Functionality	NPD	N/A	<input checked="" type="checkbox"/>
	SP500-26	3.11.2.4	Authentication and Authorization	NPD	N/A	<input checked="" type="checkbox"/>
	SP500-26	3.11.2.5	Security of Control and Comms	NPD	N/A	<input checked="" type="checkbox"/>
	SP500-26	3.11.2.6	Persistence	NPD	N/A	<input checked="" type="checkbox"/>
	SP500-26	3.11.2.7	Logging and Alerts	NPD	N/A	<input checked="" type="checkbox"/>
	SP500-26	3.11.3.1.1	Asymmetrical blocking	FW	N/A	<input checked="" type="checkbox"/>
	SP500-26	3.11.3.1.2	Port/protocol/address blocking	FW	N/A	<input checked="" type="checkbox"/>