Dell Inc.
MS. PS4-30
One Dell Way
Round Rock, Texas 78682

Re: FCC ID:	E2K-APL260AE
Applicant:	Dell, Inc.

Software Security Description		
	FCC question/requested information	**Dell | Sonicwall Response**
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	- Updates can only be obtained from Dell, Inc. secure web site (mysonicwall.com) - The legitimate user needs to register SonicWALL appliance to mysonicwall.com first. After verification using appliance serial number and authentication code, user can be authorized to download SonicOS firmware image from mysonicwall.com web portal. - After SonicOS firmware image is downloaded, administrator can login to the appliance management UI to perform firmware upgrading over HTTPS. Only Dell SonicWALL signed firmware specific to the appliance type can be used to update. All other files will be rejected.
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.	- Dell SonicWALL uses Public Key Infrastructure (PKI) to authenticate source of firmware reliably. Dell SonicWALL secure signing server uses PKI private key to sign the firmware. And Dell SonicWALL appliance has PKI public key to authenticate the firmware image. Digital Signature Algorithm (DSA) and secure hashing algorithm SHA to validate only SonicWALL signed legitimate

		firmware can be allowed for upgrading. Digest hash can ensure firmware is not modified. DSA can ensure firmware is authentic.
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	- Dell SonicWALL appliance built-in ROM Pack verifies firmware platform target to ensure firmware matches the appliance hardware product code. Only firmware dedicated for specific hardware platform is allowed for upgrading.
	5. Describe, if any, encryption methods used.	Digital Signature Algorithm (DSA) ensures firmware is authentic.
	6. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?	No, SonicWALL appliance cannot be configured as master and client.
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented?	Through the PKI, DSA and Secure hashing SHA authentication and verification. Only genuine Dell SonicWALL firmware can be accepted.
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.	No
	3. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain,	Not possible. Dell SonicWALL device sold in US can only be operated in FCC regulatory domain and US allowed frequencies. The

	frequencies, or in any manner that is in violation of the certification.	product regulatory domain identification cannot be modified by all means
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	After Dell SonicWALL device is registered, device unique Serial number and regulatory domain are tied in to backend database to prevent third party from downloading non-US versions of firmware. And device authenticates and verifies firmware signature to only allow US-versions of firmware for upgrading.
	5. For modular devices, describe how authentication is achieved when used with different hosts.	NA
SOFTWARE CONFIGURATION DESCRIPTION		
USER CONFIGURATION GUIDE	1. To whom is the UI accessible? (Professional installer, end user, other.)	UI can only be accessed through user name and password authentication. The purchaser of the appliance defines roles and how they want to manage this access and what is restricted. Nothing in the UI can set appliance outside the parameter per grant of authorization
	a) What parameters are viewable to the professional installer/end-user?6	Depends on purchaser policy.
	b) What parameters are accessible or modifiable to the professional installer?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
	i) Are the parameters in some way limited, so that the installers will not enter	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.

	parameters that exceed those authorized?	
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
	c) What configuration options are available to the end-user?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Nothing in the UI can set appliance outside the parameter per grant of authorization. No special modes for installers or professionals or user.
	d) Is the country code factory set? Can it be changed in the UI?	Appliances sold in US are set at factory for North American Domain, which restricts appliance to the parameter per grant of authorization.
	i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Appliances sold in US are set at factory for North American Domain, which restricts appliance to the parameter per grant of authorization.
	e) What are the default parameters when the device is restarted?	When device is restarted it will return to last saved setting. Only when administrator explicitly chooses to reset device configuration to factory default, device can return to default parameters.
	2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information	The Dell SonicWALL appliance radio is configured in normal BSS access point mode.

	is available in KDB Publication 905462 D02.	
	3. For a device that can be configured as a master and client (with active or passive scanning),if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?	NA
	4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))	NA

Rick Linford
Regulatory Compliance Engineer
Dell | SonicWALL
email : rick_linford@dell.com
Phone : 408.962.8798