Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Phone: 408 526-4000
Fax: 408 526-4100
http://www.cisco.com

July 16, 2010

To: **Cisco US/Canada Utility Customers**

The purpose of this letter is to provide information to Cisco's utility customers regarding certain security features in Cisco's routers, switches, firewalls, Access Control Server (ACS), Intrusion Prevention System (IPS), and Cisco's Security Monitoring, Analysis and Response System (CS-MARS).

Cisco routers, switches, firewalls, and CS-MARS run special-purpose embedded operating systems that have been developed specifically to support their intended functions. These are closed operating systems designed and built to run exclusively on these devices, and are not designed for non-administrative multi-user access.

Cisco routers, switches and firewalls have several self-protection mechanisms at runtime designed to prevent malicious code injection. The use of strong authentication and SSL standards is intended to protect the management of embedded web servers. Because of the combination of self-protection mechanisms and architectural design, Cisco routers, switches and firewalls do not include, require or support traditional anti-virus/malware agents, such as those found on general-purpose operating systems.

CS-MARS and ACS are security appliances built on top of Linux that have several self-protection features designed to make them resistant to attacks. These include a stripped-down operating system; secure administrative access; restricted commands; restricted access to the filesystem; two-part administrative password; secure shell remote access; a built-in firewall; and controlled upgrade/updates. Neither CS-MARS nor ACS include, require or support traditional anti-virus/malware agents, such as those found on general-purpose operating systems.

Cisco Intrusion Prevention System is a security-monitoring appliance built on top of Linux that has several self-protection features designed to make it resistant to attacks. These include a stripped-down operating system; secure administrative access; restricted commands; restricted access to the filesystem; two-part administrative password; secure shell remote access; and controlled upgrade/updates. IPS does not include, require or support traditional anti-virus/malware agents, such as those found on general-purpose operating systems.

Please note that the statements in this letter are merely intended to provide information regarding the features of Cisco's products, and do not constitute any warranty or binding obligation. Any such binding obligations will be contained in a mutually acceptable written agreement between the parties.

Laura Ipsen
GM/SVP
Smart Grid Business Unit