Adriel T Desautels
President, Secure Network Operations, Inc
Phone: 978-263-3829
Fax: 978-263-0033

Responding to comment No. 7

Class: All classes of copyrighted works should be exempted under certain conditions.

Argument:

All classes of copyrighted works should be exempted under certain conditions, as it is more damaging under those conditions to suppress information than it is to disclose it. The DMCA fails to clearly identify these conditions and thus enforces unreasonable information suppression.

This is particularly threatening to the security of the nations computer infrastructure that supports core of the US economy. This threat exists because malicious computer hackers are able to protect their malicious software utilities (malware) under the DMCA. This protects the malicious hackers and crackers and makes vulnerability discovery overly complex.

This threat is further enforced as it allows for vendors to deny the public disclosure of vulnerabilities discovered in their respective products, but cannot stop or hinder the private disclosure of the vulnerability. Again, this is empowering the malicious hackers and crackers and hindering the ethical computer security professionals.

The DMCA should be thoroughly reviewed and modified to include certain conditions in which information disclosure of copyrighted materials is allowed under law. The DMCA should also make a clear effort to discontinue the support of malware, and enforce the disclosure of threatening computer security vulnerabilities.

Burden Of Proof:

First Proof: (1) RedHat's recent clash with the DMCA. Malware was released by a group of hackers in binary form. The malicious hackers malware was clearly copyrighted and was protected by the DMCA. Because of this RedHat could not release a fix to anyone within US jurisdiction and the United States computer infrastructure suffered from undisclosed vulnerabilities and attacks. For a US citizen to download the patch that would resolve the vulnerability, was in fact illegal and was punishable by law (DMCA).

Second Proof: (2) DMCA can be used by a computer software or computer equipment vendor in an attempt to hide dangerous product flaws. In 2002 the Hewlett-Packard Company ("HP") threatened to prosecute and sue SNOsoft under the DMCA in an effort suppress or quash the disclosure of critical computer security vulnerabilities. Some of these same vulnerabilities were already circulating in the private malicious hacker (blackhat) community however were unknown to the ethical security (whitehat) community or to the companies running the vulnerable software. This is another example of how the DMCA threatens the US network security infrastructure and can be used to unknowingly support illegal and malicious activities.