SOFTWARE FREEDOM LAW CENTER
1995 Broadway, 17th Floor
New York, NY 10023
212.580.0800
212.580.0898 fax
www.softwarefreedom.org

February 28, 2006

Sarbanes-Oxley and the GPL: No Special Risk

Some have recently argued that corporate executives face increased risk of criminal liability under the Sarbanes-Oxley Act of 2002 (SOX) if their companies develop and distribute code licensed under the GNU General Public License (GPL). The argument, as it has been made, raises significant concerns about SOX compliance, but it fails to clarify the scope and context of these points. We have reviewed these issues and, as discussed more fully below, there is in fact no special risk for developing GPL'd code under SOX. Under most circumstances, the risk posed to a company by SOX is not affected by whether they use GPL'd or any other type of software. Arguments to the contrary are pure anti-GPL FUD.

First, SOX only applies to companies that are required to file periodic reports with the Securities and Exchange Commission (SEC). This includes companies that have filed registration statements to offer securities to the public, companies that list their securities on stock exchanges or companies that register their shares and become subject to continuing SEC reporting requirements because they have more than $10 million in assets, 500 or more shareholders worldwide and, in the case of foreign private issuers, 300 or more shareholders resident in the United States. Other companies are not subject to SOX at all.

Second, the SOX certification and internal controls regulations are qualified by materiality standards. If a company's reliance on a license to software is not material and if it reasonably believes that any harm from a violation of the license is not substantial, then nothing about the use (or misuse) of that software would rise to the level requiring disclosure in the company's periodic reports. Similarly, any incorrect disclosure of a non-material statement in the company's reports would not run afoul of the SOX certifications.

Historically, GPL violations have not triggered massive lawsuits for damages the way that violations of proprietary license agreements have. The primary enforcer of the GPL is the Free Software Foundation (FSF), who has never used a GPL violation as the basis to go to court to seek a large damage award or enjoin software distribution. The FSF's stated policy is to ensure compliance, not to prevent software distribution or to seek damages.

What this means practically for the vast majority of companies complying with SOX is that the threat to their businesses posed by potential GPL license violations, both inadvertent and intentional, is so low as to be immaterial. In any case, the financial impact of GPL violations is likely to almost always be lower than the impact of proprietary license violations, for which parties routinely bring suit for damages.

Third, companies subject to SOX must bear the cost of full SOX compliance whether or not they use software distributed under GPL. Some have claimed that even companies complying with the GPL violate federal law if they do not require legal department review of all GPL compliance. This is an overstatement, as companies that do not have adequate internal controls are in violation of the securities laws regardless of whether or not they use GPL'd software, non-GPL'd software, or no software at all. Inadequate compliance with any license that is material to the company would be problematic under SOX. The same analysis is applicable to companies that use any code that they do not have the rights to use, which would include improper use of proprietary software as well as free and open source software.

In most instances, compliance with proprietary licenses is much more complex than GPL compliance because the GPL is a general license with obligations that are fairly simple and understandable. No money changes hands, seats are not counted, and licenses are not time-limited. GPL compliance is a fairly simple matter, and if a company has concerns about how to comply, the FSF is staffed with experts who can and do help companies create efficient compliance procedures. Proprietary licenses, on the other hand, often contain both a greater number of provisions and a greater complexity than the GPL. Thus, a company trying to understand its rights and comply with its obligations under such a complex and detailed license will have a much harder time than one who must merely comply with the GPL. Accordingly, the risk of inadvertent license violation is often greater with non-GPL licenses.

Fourth, the provisions introducing criminal penalties under this part of SOX contain a scienter element. Section 906 imposes criminal liability upon certifying executives who “knowingly” or “willfully” falsely certify. While these executives are required to implement adequate controls to determine compliance, to the extent that they do not knowingly or willfully make the false certification they are not subject to criminal liability under SOX. The dangers of accidental criminal liability under SOX are no greater for GPL'd software than for non-GPL'd software.

Companies subject to SOX should take their reporting and certification requirements very seriously. It is important that such companies understand their obligations and ensure that they are not in violation of any licenses or any other restrictions related to intellectual property. While GPL compliance can be an important part of this analysis and compliance with SOX, risks associated with the use of GPL software should be considered in the full context of securities law compliance. In the

end, contrary to what others may argue, there is in fact no additional SOX liability or risk for using GPL software.