[Proposed class or classes of copyrighted work(s) to be exempted]= Class 1: Literary works, sound recordings, and audiovisual works accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

Or, in the alternative:

Class 2: Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

[Brief summary of the argument(s) in support of the exemption proposed above]= Since the third rulemaking, evidence has been uncovered indicating that security flaws in technological protection measures ("TPMs") affecting works outside the scope of the sound recording exemption granted by the Librarian have created similar security vulnerabilities in many more PCs. A flaw uncovered last year in Macrovision's SafeDisc software, one of the most widely used copy-protection systems for PC-accessible video games, exposed PCs to attacks similar to but even more dangerous than those enabled by the Sony rootkit. Because SafeDisc shipped preinstalled on nearly every copy of the Microsoft Windows XP and Windows 2003 operating systems, the vulnerability affected nearly one billion PCs, two thousand times more than the rootkit.

Serving as another prominent example of this kind of TPM is Sony's SecuROM software, utilized by dozens of high-profile video game publishers including Atari, Bethesda Softworks, Capcom, Eidos, Electronic Arts, Konami, LucasArts, Microsoft, Sega, and Ubisoft. PC-accessible video games utilizing SecuROM automatically install copy-protection software, often without the consumer's knowledge. Independent security experts have not yet rigorously studied SecuROM; in the absence of a definitive analysis, anecdotal contentions of harm, speculation about causes, and contradictory assessments of risk have run wild on the Internet. While Sony maintains that the TPM is safe, some users report that it disables critical system security functionality including firewalls and antivirus software, opening their PCs to a variety of viruses, spyware, and other malware. Three class action lawsuits have been filed against Electronic Arts on behalf of those allegedly negatively affected by the incl! usion of SecuROM in the popular video games Mass Effect, Spore, and Spore Creature Creator.

Whether or not SecuROM causes actual security vulnerabilities, the uncertainty about its risks has created an environment of suspicion where consumers fear the worst. Given the immense stakes that users hold in the security of their PCs - private communications, valuable data, and even financial assets vulnerable to theft and fraud - the presumption that SecuROM is insecure may be a rational decision to err on the side of caution. Yet, consumers who bought SecuROM-encumbered games unaware of the potential risks are now placed between a rock and a hard place, forced to choose between accepting the indeterminate risks posed by SecuROM and abandoning access to their lawfully obtained video games. This is an unacceptable proposition for consumers.

Furthermore, the SafeDisc and SecuROM fiascos showcase the very real chilling effect of the DMCA anti-circumvention measures on security research related to these TPMs. Even though SafeDisc exposed hundreds of millions of PCs to a serious security vulnerability, over six years passed after the release of the TPM until anyone but attackers knew about the vulnerability, which was not publicly documented until a security researcher observed a piece of malware exploiting it. And the ongoing uncertainty over SecuROM's safety could probably be settled by a single definitive scientific study; instead, a regime of panic, protests, and litigation has taken hold over what may turn out to be nonexistent or easily reparable faults.

Despite the high stakes, security researchers have clearly avoided addressing these problems, and the chilling effect of the DMCA anti-circumvention provisions is at least partially to blame. Security researchers remain the last defense against dangerous security flaws caused by TPMs, and discouraging their intervention is completely undesirable. Accordingly, an exemption to the anti-circumvention measures is needed to allow security researchers to investigate and fix security flaws caused by TPMs on PC-accessible video games, and for consumers to apply those fixes to access their lawfully obtained games.

A growing body of evidence suggests an inherent tension between digital rights management ("DRM") technology embodied by these TPMs and user security. Accordingly, we can confidently predict that the Sony rootkit, SafeDisc, and SecuROM will not be the last TPMs to cause collateral security harm. The exemption of Class 2 from the anti-circumvention measures should be adequate to mitigate the harms caused by TPMs that control access to PC-accessible video games because it will remove the chilling effect of the anti-circumvention measures, thereby encouraging independent researchers to investigate and correct security flaws in these TPMs and allowing users to stay informed and take appropriate measures to protect themselves.

However, potentially dangerous TPMs will likely be used on many other PC-accessible works between now and the next rulemaking procedure in 2012. To wit, TPMs are being used (or are planned for use) on ebooks and

digitally distributed multimedia content. The continued use of flawed TPMs in the aftermath of the Sony rootkit fiasco indicates that the risk of harming consumers is unlikely to provide the content industry with sufficient incentive to be diligent about security, and those consumers should not be forced to wait years to gain secure access to their lawfully obtained works. Accordingly, an exemption of Class 1 from the anti-circumvention measures is needed to prospectively allow security researches to discover and fix security flaws in other PC-accessible works before attackers find and exploit these flaws against consumers.