Opening Statement of

Tim Schaaff

President of Sony Network Entertainment International

Before the Senate Commerce, Science and Transportation Committee

Washington, DC

June 29, 2011

Chairman Rockefeller, Ranking Member Hutchison, and other distinguished members of the Committee, thank you for providing Sony with this opportunity to testify on cyber crime and data security.

My name is Tim Schaaff, and I am President of Sony Network Entertainment International, a subsidiary of Sony Corporation.

I am chiefly responsible for the business and technical aspects of Sony's PlayStation Network and Qriocity, online services that allow consumers to access movies, television shows, music and video games.

As you know, this year, Sony has been one of a growing number of targets of an increasingly common digital-age crime: a cyber attack.

Almost every day it seems a new story emerges about businesses, government entities, public institutions and individuals becoming victims of this cyber crime wave; thus, supporting President Obama's statement noting that these cyber attacks are "one of the most serious economic and national security threats our nation faces." This warning was recently echoed by Defense Secretary Gates, "[t]here is a huge future threat and there is a considerable current threat [from cyber attacks]. That's just a reality we all face."

If nothing else, perhaps the frequency, audacity and harmfulness of these attacks will help encourage Congress to enact new legislation to make the Internet a safer place for everyone to learn, enjoy entertainment and engage in commerce. We applaud this Committee for its work on the issue, and we stand ready to assist you in whatever way we can.

Regarding the attack on Sony, please let me briefly provide some details. Initially, Anonymous, the underground group associated with last year's WikiLeaks-related cyber attacks, openly called for and carried out massive "denial-of-service" attacks against numerous Sony Internet sites in retaliation for Sony bringing an action in federal court to protect its intellectual property.

During or shortly after those attacks, one or more highly skilled hackers infiltrated the servers of the PlayStation Network and Sony Online Entertainment.

Sony Network Entertainment and Sony Online Entertainment have always made concerted and substantial efforts to maintain and improve their data security systems. A well-respected and experienced cyber-security firm was retained to enhance our defenses against the denial-of-service attacks threatened by Anonymous. But unfortunately no entity – be it a mom-and-pop business, a multinational corporation, or the federal government – can foresee every potential cyber-security threat.

On Tuesday, April 19, 2011, our network team discovered unplanned and unusual activity taking place on four of the many servers that comprise the PlayStation Network. The network team took those four servers off line and an internal assessment began.

On Wednesday, April 20th, we mobilized a larger internal team to assist in the investigation. And on that date, the team discovered the first credible indications that an intruder had been in the PlayStation Network system. We immediately shut down all of the PlayStation Network services in order to prevent additional unauthorized activity.

That same afternoon, a security firm was retained to "mirror" the servers to enable a forensic analysis. The scope and complexity of the investigation grew substantially as additional evidence about the attack developed.

On Thursday, April 21st, a second recognized firm was retained to assist in the investigation.

On Friday, April 22nd, we notified PlayStation Network customers via a post on the PlayStation Blog that an intrusion had occurred.

By the evening of Saturday, April 23rd, we were able to confirm that intruders had used very sophisticated and aggressive techniques to obtain unauthorized access to the servers and hide their presence from the system administrators.

On Sunday, April 24th, yet another forensic team with highly specialized skills was retained to help determine the scope of the intrusion.

By Monday, April 25th, we were able to confirm the scope of the personal data that we believed had been accessed. Although there was no evidence credit card information was accessed, we could not rule out the possibility.

The very next day – Tuesday, April 26th – we issued a public notice that we believed the personal information of our customers had been taken and that, while there was no – and there still is no – evidence that credit card data was taken, we could not rule out the possibility. We also posted this on our blog and began to email each of our account holders directly.

On Sunday, May 1st, Sony Online Entertainment, a multiplayer, online video game network, discovered that data may have been taken. On Monday, May 2nd, Sony Online

Entertainment shut down this service and notified customers that their personal information may have been compromised.

Throughout this time, we felt a keen sense of responsibility to our customers:

- We shut down the networks to protect against further unauthorized activity;
- We notified our customers promptly when we had specific, accurate and useful information;
- We thanked our customers for their patience and loyalty and addressed their concerns arising from this breach with identity theft protection programs – at no cost to consumers – for U.S. and other customers (where available) and a "Welcome Back" package of extended and free subscriptions, games and other services; and
- We worked to restore our networks with stronger security to protect our customers' interests.

We have relaunched our networks, with stronger security protections in place, and we are pleased that our customers have been very loyal and excited about returning to them. In fact, our PlayStation Network activity level is already up to more than 90 percent of what it was before the attack. And sales of our PS3's are up double-digits this year.

Two final points. First, as frustrating as the loss of the network for playing games was for our customers, the consequences of cyber attacks against financial or defense institutions could be devastating for our economy and security. Consider the fact that defense contractor Lockheed Martin and the Oak Ridge National Laboratory, which helps the Department of Energy secure the nation's electric grid, were cyber attacked within the past several months. Even the CIA, the FBI and the U.S. Senate have recently experienced such attacks.

Second, we support federal data breach legislation that would: (1) provide consumers – regardless of what state they live in – the assurance that if and when their personal data is compromised, they will receive timely, meaningful, and accurate notice of this fact; (2) ensure that consumers receive helpful information on what measures they can take to mitigate any potential harm, including free credit reporting in cases in which such a service is warranted; and (3) treat all similarly situated companies that possess personal information equally.

By working together to enact meaningful cyber-security legislation, we can limit the threat posed to us all. We look forward to working with you to ensure that consumers, businesses and governments are empowered with the information and tools they need to protect themselves from cyber criminals. We are willing and eager to help provide law enforcement with the laws and resources they need to prevent cyber crime from occurring and bring cyber criminals to justice when prevention fails. And by simultaneously moving forward on data breach policies and legislation, we can ensure

that consumers are empowered with the necessary information and tools to protect themselves from these cyber criminals.

Thank you.