2211 North First Street, San Jose, CA 95131

August 1, 2011

Mr. Jon Boyens
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Mail Stop 893
Gaithersburg, MD 20819

VIA EMAIL: SecurityGreenPaper@nist.gov

Dear Mr. Boyens and the Internet Policy Task Force:

PayPal welcomes the opportunity to provide comments on the Department of Commerce Internet Policy Task Force's Green Paper on Cybersecurity, Innovation, and The Internet Economy. PayPal is a leading online payments company, with more than 94 million active user accounts internationally, supporting payments in 25 currencies. Headquartered in San Jose, California, PayPal has offices in several states in the United States, along with its international headquarter in Singapore and European headquarter in Luxembourg. PayPal's payments solution connects into and leverages the traditional payment networks (whether ACH, bank card networks, or PIN networks) enabling its users to make and receive payments in a safe, efficient and cost effective manner.

With the White House as well as several Departments and Agencies publishing various cyber-strategies as well as requesting input and comment on cyber-related issues, the publication of this paper and the call for comments is timely. Coordination among the various government agencies is extremely important, given the time necessary to develop a comprehensive informed opinion. In addition, a Federal-level coordinated effort would facilitate a multidisciplinary approach to cybersecurity that is essential for long-term success.

The Internet has proven remarkably resilient with its transformation from academic experiment to an essential component of the global communications infrastructure and economy. Few if any industries are exempt from change wrought by the Internet or the services built on top of it. While change can be disruptive, it also presents an opportunity for improved and/or enhanced services. In large measure, the changes brought about through the Internet have been overwhelmingly positive.

The pace of change and innovation, especially in the last 10-15 years, has been dramatic and perhaps is accelerating. Where once only the most innovative, technologically advanced, and forward thinking companies considered the Internet integral to business development, now even small and medium sized industries feel

compelled to have an Internet presence. Given the decline in print publication readership and consumers' increasing reliance on Internet search for phone numbers and service selection, even small, local businesses now have an Internet presence.

Having a single, open, generative communication medium with the well-documented power of the Internet is driving innovation; in ways large and small, for good and evil. With the move of commerce from bricks and mortar to wireline and wireless, the global community has seen a similar migration of crime. In the physical world, crime is relatively well understood as are security measures that can be taken by entities, large and small, to mitigate threats and losses. Sadly, crime on the Internet is generally less well understood, except by cybersecurity practitioners, and as a consequence many commercial entities, both large and small, are seriously at risk and are ill-prepared to defend against theft or (criminal) cyber attack.

Compounding the problem is a lack of qualified cyber law enforcement experts. In the physical world, there are both pro-active and reactive law enforcement activities; witness police patrols and detectives investigating crimes after the fact. In the virtual world, there is a lack of the deterrent effect of patrols and law enforcement is woefully understaffed on the investigative front. While a deterrent presence is warranted, it should not come from law enforcement. Rather, this may be where the most forward thinking I3S members could play a substantial beneficial role.

In the current economic environment, some law enforcement agencies are in fact reducing their investments in cybercrime units. We have anecdotal evidence that in some local jurisdictions, high-tech units are being disbanded in favor of relying on regional, state, and federal resources. Unfortunately, states and the federal government are experiencing unprecedented budget pressures themselves and are therefore unlikely to be able to handle any increased workload. In fact, the recent federal budget "compromise" will likely increase pressures on all departments, including law enforcement, to reduce spending. A reduction in, high-tech investigative resources, especially in an environment with little or no deterrence is a "perfect storm" for increased criminal activity and economic harm to individuals and corporations.

It is well-known that criminals engage in and have very effective information exchange, substantially enhancing their return on investment. I3S members have discussed information sharing for many years but have made little progress towards developing a comprehensive plan. Legal obstacles are primarily to blame for the lack of progress and a concerted effort to clear them might enable a core group of committed innovators to meaningfully share information (and best practices) enabling legal deterrent actions without compromising individual rights or privacy.

The Department of Commerce (Department) might be the focal point for such an effort though we caution against a governmental entity serving as a collection and dissemination hub. Industry can best develop and act in that capacity, perhaps with thoughtful regulatory oversight. Regulatory direction or safe harbor legislation would be required for industry to advance down this path. We encourage the Department to coordinate with the Department of Justice to ensure that deterrent and investigative activities are aligned and therefore providing maximum benefit.

We are encouraged by the recognition of I3S but believe that it is perhaps a much broader segment than that envisioned by the authors of the green paper. Using the definition given in the paper, we believe that any entity

connected to the Internet qualifies for inclusion in the I3S. This is a very large sector indeed and consequently would be very difficult to "target" and reach. Within the defined sector, there are a number of innovative and influential companies with the requisite skills and motivation to offer both expertise and assistance in defining appropriate security measure and best practices for any Internet-connected entity. Without offering a specific definition of this group, we suggest that the Department would be well-advised to develop such a definition and to seek multi-stakeholder participation in developing cybsercurity best practices.

Any entity that connects to the Internet, regardless of size or level of innovation, has a responsibility to employ best practices. Rather than target only "innovators", a somewhat different approach would look at the types of services provided, and to develop best practices around those services. For example one possible taxonomy is: provides information (no data collection), provides information (collects data), collects PII, collects sensitive PII, provides user access to data, etc.

By way of example, a site that is "read only", a mapping service, would follow one set of practices designed to ensure that its information was not improperly modified and that its services were resistant to a variety of well-known attacks, e.g. DDoS. A site that collects and stores information for later reuse, perhaps by storing a "state" cookie on a user's machine, would enhance those practices with additional mechanisms to protect against "theft" of server-side information accessed via that cookie. Sites that collect more and/or more sensitive data should follow yet more stringent standards as should sites that house significant amounts of data, regardless of the sensitivity.

These practices should be followed regardless of the scale of the entity or level of "innovation". There should be no distinguishing between a multi-billion dollar international industry and a small enterprise that both house vast amounts of information possibly of a sensitive nature. Both must employ practices designed to safeguard the information itself and the services designed to provide access to it.

In addition to service providers, it is essential that a set of best practices for service consumers is established. Any device attached to the Internet can serve as the source of a cyber threat and while it is impossible to eliminate that threat, mitigation is within our reach. Many of today's cyber attacks are a result of malware being distributed to and activated on "remote" machines. Viruses, worms, bots, and other forms can be detected and eliminated if individuals followed industry best practices for personal computers. Unfortunately, too few people are aware of or follow these practices and as a consequence, an alarming number of machines are infected making them potential sources for identity theft, account takeover, or DDoS among others.

Consumers must be educated about the threats they are exposed to via the Internet. Education efforts should begin early and continue through college and advanced degree programs, with age-appropriate material at each level. At the university level, we need more and better attention paid to security in the development of programs, websites, and other Internet-accessible services. The Department should work with the Department of Education to develop plans and initiatives that are aligned with other Federal activities in this space. A comprehensive program, as outlined here, is necessary to provide the educational background required for individuals to make appropriate, well-informed decisions regarding security online, as they grow and mature. To develop and maintain such a program will require involvement by expert curriculum designers as well as

cybersecurity professionals, and it is our belief that the Department of Education is likely the best owner of this initiative, rather than any other government Department.

The diverse nature of the threat landscape as well as the complexity in legally dealing with those threats demands a coordinated response. PayPal has written a white paper *COMBATING CYBERCRIME: Principles, Policies, and Programs*[1] that lays out a set of principles for establishing such a coordinated response. The policies and programs presented in this PayPal paper represent a framework for comprehensively addressing cybersecurity.

Thank you for the opportunity to provide comments on this important topic. If you have any questions or would like to discuss any of the issues raised herein, please do not hesitate to contact me.

Sincerely,

Michael Barrett

Chief Information Security Officer, PayPal

[1] https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf