PayPal

2211 North First Street
San Jose, CA 95131
TEL 408 967 1000

September 20, 2010

Ms. Dian Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Via e-mail to: cybertaskforce@doc.gov

RE: United States Department of Commerce, Notice of Inquiry
Cybersecurity, Innovation and the Internet Economy
Docket No. 100721305–0305–01

Dear Ms. Honeycutt:

PayPal, a leading global online payment company, is pleased to submit comments in response to the United States Department of Commerce's (herein, "Department") Notice of Inquiry (NOI) on Cybersecurity, Innovation, and the Internet Economy.

PayPal firmly shares the Department's position on cybersecurity, namely that the Internet is an ever more critical resource to the global economy and people's lives, and that preserving an open, innovative, generative Internet is an important goal. We also share the belief that without improvements in the fundamental governance and security of the Internet, it cannot continue to fulfill its promise. Improvements in cybersecurity must not be viewed as a competitive advantage or differentiator. Improving cybersecurity must treated as a collective goal; a common good. A rising tide that lifts all boats.

At least today, we believe that policy development in the area of cybersecurity is difficult. Two reasons in particular are noteworthy:

1. In the US, there are still role/responsibility questions between agencies which have not yet been resolved; and
2. Even if all policy questions are resolved domestically, the Internet is a fully global infrastructure, and thus whatever policies responses are utilized in the US generally have to be capable of being replicated at global scale.

PayPal

2211 North First Street
San Jose, CA 95131
TEL 408 967 1000

PayPal operates with several cybersecurity basic principles in mind:

- Cybercrime, particularly phishing, malware and identity fraud, is the biggest threat to the continued development of the online economy. The success of the Internet ultimately rests upon consumers trusting the Internet and its safety. Cybercrime erodes this trust, and if unchecked could destroy it.
- At PayPal we regard fighting cybercrime as a strategic business priority. We invest heavily in keeping our sites and services safe and secure, and in detecting and preventing fraud. Our efforts are complemented by close cooperation with law enforcement around the globe.
- Our government relations team engages regularly with policy makers to share our expertise and ensure there is an effective legal framework and commitment to fighting cybercrime domestically as well as internationally.
- Cybersecurity solutions must require that those best able to provide for security be held responsible and accountable for doing so.

Quantifying the Impact

PayPal supports the proposal to gather and report more uniformly on key economic indicators related to cybersecurity. Current reporting schemes are mostly unreliable because they rely on both voluntary reporting of data and on non-standard terminology that is neither uniform across industries, nor even within a given industry. While considerable private industry data exists on the problem, the reported losses from cybercrime cannot be compared from one study to another. The ranges of losses varies wildly, ranging from low numbers of billions of dollars, and at least a couple of estimates into the trillion dollar range. We believe that these upper estimates are not credible, and we suspect that the lower ones are in fact under representing the scale of the problem.

Government can and should play a strong role in the centralized collection and dissemination of cybercrime data. Multiple hurdles exist to uniform reporting but the ultimate value from the consolidated numbers far outweighs the challenges of implementation. Just as certain FBI statistics reveal much about the overall levels of other types of crimes, uniform and universal reporting and dissemination of cybercrime information will paint a much clearer picture of where the biggest problems are, and where the most energy should be expended.

Any analysis of the economic impact should cover both the direct losses, and the current security spending necessary to sustain the status quo must be a part of any reporting system. The challenges include the standardization of terminology and a common taxonomy for the field, as well as a lack of mandatory reporting. Because of statutory minimums in laws such as the Computer Fraud and Abuse Law (CFAA), many cybercrimes that fall under the threshold go unreported to the United States government. In many cases these crimes go unreported to any law enforcement agency and are therefore unquantifiable.

2211 North First Street
San Jose, CA 95131
TEL 408 967 1000

There are currently no incentives for businesses to report cybercrimes that do not fall under breach disclosure rules, or that cannot be meaningfully investigated and prosecuted. These smaller crimes in aggregate may represent a substantial portion of the overall cybercrime landscape, but there is generally a blindness to the activity because of a lack of mandatory reporting. The other obstacles to reporting are privacy/liability concerns. Without privacy guarantees such as those granted through the Information Technology-Information Sharing and Analysis Center (IT-ISAC), neither large enterprises not currently part of an ISAC, nor a small or medium business will be able to report cybercrimes with confidence that the data will not be disclosed.

As indicated previously, data on the current costs of security measures is critical. Many security and fraud incidents are stopped through the use of existing security measures. The associated costs appear on balance sheets but the attacks they have prevented do not. Having a better understanding of the costs of existing security and fraud controls will be of utmost value in determining the appropriate areas in which to focus attention.

Once accurate data exists as to the scale of the problem, in terms of how much money consumers and companies lose through cybercrime, the obvious next question is what can be done to solve it. We believe that it's necessary to understand where the stolen money is ending up, and whether some countries and regions have a relatively disproportionate share of the global profits. Of course, such a geopolitical analysis may be comfortably beyond the remit of the Department, but nonetheless this analysis does need to be performed.

Raising Awareness

Increased education and awareness are important components in any coordinated effort to improve cybersecurity. However, caution is urged against over-reliance on these consumer tactics and expecting any significant short-term impact. A properly scoped campaign targeted at businesses, government agencies, universities, and other influential organizations could more reasonably be expected to show results in the near term. The technology industry should mirror the effectiveness of other public awareness campaigns such as: "Only you can prevent forest fires;" and "Click it or ticket." This is the intention behind the impending National Cyber Security Alliance (NCSA) industry campaign "Stop. Think. Connect."

Education is a critical component of a comprehensive plan. In particular, we believe that there should be a robust K-12 curriculum which covers both cyber-safety and cybersecurity. To date, most of the focus on cyber education has focused on utility and cyber-safety, with little or no emphasis on cybersecurity. There has been some academic research into what such a larger curriculum might contain, but even this work has been piecemeal. We believe that this work should be expanded and potentially incorporated into national curriculum templates.

There is a generally accepted belief that, at present, cybersecurity is not seen by consumers as a significant driver for purchasing decisions. Today, all auto manufacturers compete at some level on providing the most cutting edge safety features. This industry commitment could initially be attributed

2211 North First Street
San Jose, CA 95131
TEL 408 967 1000

to government intervention and enforcement, but is now driven consumer demand. Any education program should have as an underlying goal increasing consumer demand for products that display desirable cybersecurity features. As has been the case with auto-safety raising awareness about cybersecurity, with the appropriate education and accurate information, consumers will make informed decisions.

Web Site and Component Security

PayPal is a strong supporter of the need for overall improvements in the web security ecosystem and improvements in web security will reduce the spread of malware. However, improving web security practices will more importantly result in a reduction in other types of cybercrime including identity theft.

The existing private and public cooperation in this area is already making substantial progress in improving the ecosystem with efforts such as the collaboration at the Department of Homeland Security (DHS) on the "Build Security In" program , work done in standards organizations such as the Internet Engineering Task Force (IETF) and the world Wide web Consortium (W3C), and open source organizations such as The Open Web Application Security Project (OWASP) and the Web Application Security Consortium (WASC).

Product Assurance

Though PayPal's products are not typically covered by product assurance criteria, we believe that flexible product assurance criteria are critical to a secure ecosystem. Previous efforts to define product assurance criteria and the associated testing and certification processes have often been inflexible and too rigid with respect to technology updates including patches. The ecosystem impact has been that the highest security requirement systems are unable to apply critical security patches without a lengthy recertification process - leaving precisely those systems most critical to security with the fewest defenses. Improvements in product assurance must be made to ensure that the systems that require the higher assurance can maintain that security posture over time.

Research and Development

The lack of reliable security incident data is the biggest impediment to improvements in the state of cybersecurity. Without access to incident data, researchers, companies, and individuals are not able to do research and make meaningful choices about the security technologies they deploy. We believe that advancements in metrics and analysis of incident data and determining what works and does not work in the field of cybersecurity will provide the biggest benefit to the ecosystem.

Summary

As we noted in our introductory comments, assuring the future security of the Internet will take coordinated policy action, both within the US and outside it. That said, we believe that the stakes are high. While it isn't yet a situation of "the sky is falling", as Chicken Little famously said, it's clear that cyber-crime is slowly worsening, and there is no sign that enough remedial steps have been taken to

PayPal

2211 North First Street
San Jose, CA 95131
TEL 408 967 1000

reverse that trend. Over the long haul, systemic action will need to be taken. The steps that we've laid out in this document represent some of the ones which we believe are needed.

Thank you for allowing PayPal to share these comments. As the Department works through this process, we would be pleased to provide any additional information and insight deemed relevant to assisting your work.

Sincerely,

Michael Barrett
Vice President – Information Risk Management
Chief Information Security Officer