Rapid7 Response to Department of Commerce Internet Policy Task Force

Re: request for comment on non-legislative multi-stakeholder processes on cybersecurity issues in the digital ecosystem

Rapid7 is a security data and analytics software and services company that helps organizations around the world understand and manage their risk posture, as well as detecting and responding to security incidents. We believe that it will take focused, ongoing collaboration between the Government, private sector, and the security research community to make meaningful progress in addressing the growing cybersecurity challenges that face consumers and businesses. As such, we support the Internet Policy Task Force's suggestion of launching multi-stakeholder processes. Below we have identified two of the projects proposed by IPTF that we particularly recommend and would like to join.

Web Security and Consumer Trust:

(i) Cybersecurity and the Internet of Things. As the Internet of Things matures and more systems integrate information technologies (IT) and operational technologies (OT), cybersecurity is enmeshed in a broader risk context that includes safety, reliability, and resilience. How can we foster the emergence of voluntary policy frameworks, informed by market dynamics, that enable Internet of Things innovation while addressing the full spectrum of risks associated with cyberphysical systems?

The Internet of Things is converging the virtual and physical worlds in a way that moves the risk discussion around cybersecurity out of the realm of information and identity, into a sphere of potential physical harm. This is a new frontier of technological innovation, and will open new avenues for entrepreneurship and drive economic growth. We must not curb these benefits; yet the technology is complex and evolving fast, and we must identify ways to build security into the discussion. The best means of tackling this challenge may be to develop best practices that can be adopted by IoT organizations of all sizes. Doing so requires a collaborative effort from experts in the fields of business leadership, device development and manufacture, cyber security, and others.

There are some initiatives that have already begun on this front. BuilditSecure.ly is a volunteer effort from the cybersecurity community that works with small IoT startups to help them build security into their development and business processes. Similarly, I Am The Cavalry is a grassroots effort to connect security research expertise with industry leaders and influences to create and promote "cyber safety." In 2014, the group published the Five Star Automotive Security Program – a recommended set of five best practices to help car manufacturers build security into their process. The Open Garages project aims to help car enthusiasts understand today's modern vehicles as they adopt increasingly complex systems.

References:

http://builditsecure.ly/

https://www.iamthecavalry.org/domains/automotive/5star/

http://opengarages.org/index.php/Main_Page

Business Process and Enabling Markets:

(l) Vulnerability Disclosure. The security of the digital economy depends on a productive relationship between security vendors and researchers of all types who discover vulnerabilities in existing technology and systems, and the providers, owners, and operators of those systems. How can stakeholders build on existing work in this space to responsibly manage the vulnerability disclosure process without putting consumers at risk in the short run?

There is currently a great deal of discussion about how the US can effectively defend against the growing cybersecurity threat. Many of the approaches being discussed focus on addressing the symptoms of this threat; few focus on the underlying issues that create opportunities for attackers, and how we can reduce them. Identifying, investigating, and disclosing vulnerabilities in technical systems is a key step towards reducing these opportunities and mitigating attacks. However, the culture around disclosure is still evolving, and currently the majority of organizations are unprepared for a disclosure, while security researchers still disagree on correct approaches. We must create best practices and drive adoption in both the vendor and researcher communities in order to reduce the number of opportunities for attackers. It's time to apply "See Something, Say Something" to our technical systems.

It's time the various related parties came together to reach consensus on best practices for behavior on both sides of the equation. There have been previous attempts in both camps to do this, but to the best of my knowledge, no recent unified attempt across both vendors and researchers. In addition, the cybersecurity landscape is changing quickly and any existing efforts in this area are now out of date. Headlines driven by numerous high profile breaches and broad-reaching vulnerability disclosures have created a greater sense of awareness and concern over security in business leaders, opening the door for this kind of initiative. There is a richer ecosystem in this area now, and any efforts in this area should not only include vendors and researchers, but also bug bounty companies, vulnerability handling and classification entities such as CERT/CC and MITRE, legal experts in this area, and others.

References:

http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231

http://searchsecurity.techtarget.com/video/Katie-Moussouris-of-Microsoft-on-vulnerability-disclosure-ISO-standard

https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf

https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00