Request for Comments on F.R. 2015-06344

The Internet Infrastructure Coalition ("i2Coalition") submits these comments in response to the March 19, 2015 Federal Register notice 2015-06344 requesting public comment on certain issues raised by the Department of Commerce Internet Policy Task Force ("IPTF"). The IPTF seeks to identify areas related to cybersecurity, the digital ecosystem, and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers. We first provide general comments in the Overview and General Principles section, followed by more directed feedback related to the specific questions under consideration by the IPTF.

Overview and General Principles

The Internet community is working to accommodate both its desire for seamless connectivity and communication, with recognition of the fact that there are those who seek to use this fact to act in ways that are different from established Internet norms, and are in some cases illegal.

The I2Coalition recognizes that government has an important role to play in cybersecurity. That role, must, however, accommodate the processes and procedures that have led to the most powerful engine for economic growth, and communication, seen in many generations. The I2Coalition rejects a "balancing" approach to Internet security. We believe that security need not come with the cost of decreased innovation, business activity, or exercise of fundamental human rights. We propose the following general principles to guide future governmental decisions and law-making.

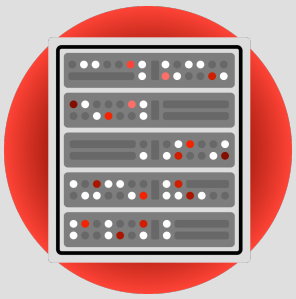
Technology has created a platform for a truly global marketplace. Non-collaborative decision-making and regulation carries with it a high risk of exclusion.
Strong regard for the security and privacy of end users builds trust in the companies with whom those end users choose to do business.
Private companies and organizations have a passionate and vested interest in solving the growing threat of cyberattacks. They should be encouraged and supported in this goal.
Encouraging innovation and economic potential should be at the center of decisions made about cybersecurity, . Two ways of insuring this are investment in education and support for innovative business ideas.

What additional collective steps can be taken to support efforts to create awareness and manage the effects of botnets? How can stakeholders build on existing work to responsibly manage the vulnerability disclosure process without putting consumers at risk in the short run?

Information sharing is widely seen as a logical next step in mitigating cyberattacks. To be effective, information sharing with the government must: (i) encourage broad participation; (ii) provide useful information to the future targets of any cyberattack; and (iii) be narrowly tailored to avoid abridging fundamental Constitutional rights. A private company will not be encouraged to participate in any information sharing program if by doing so it subjects its customers to undue scrutiny, subverts the security or privacy of their data or is seen by customers as back door surveillance. Equally as important, if adequate information isn't shared down, companies will not be any stronger or better prepared to deal with future attacks that fit a currently known profile or pattern.

The sharing of situational awareness of botnet activity by private companies can be facilitated in a number of ways. For example a botnet "war room", with an invitation to contribute validated data stripped of personally identifying information could make identifying trends and patterns easier for security researchers.

INTERNET INFRASTRUCTURE COALITION



718 7th Street NW
2nd Floor
Washington DC 20001

staff@i2coalition.com
(202) 780-7237

What collective action can be taken to promote the voluntary adoption and diffusion of existing technical solutions (e.g., DNSSEC, BGPSec and RPKI, DANE and certificate transparency) to make the internet's core infrastructure more trustworthy? What actions can improve web security and trust for consumers?

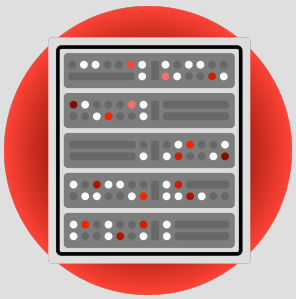
The government should support companies that adopt strong default security practices, such as SSL, and the ability for customers to protect their data in the manner best suited to them. Weakened security and backdoors for the benefit of law enforcement agencies is incompatible with the goal of bolstering the security of core infrastructure. Sophisticated, motivated criminals will always discover a built-in security hole. The U.S. government should continue its strong tradition of facilitating security choices important to business, understanding that there is not a "one size fits all" security solution. It is important to recognize that in the past four years the customers of Internet companies have spoken: the Internet economies of countries who support network security will grow; those who do not will shrink. Government support should be clear and consistent: strong security is better for everyone. Educational efforts that promote good security practices, including the adoption of the methods specified, will help. Rating and evaluation schemes, if promulgated and validated, will help consumers choose relatively more secure solutions and drive adoption.

How can diverse stakeholders work together to limit the risk of malvertising? Are there best practices and existing standards that providers of online applications and downloadable tools can adopt to ensure consumer protection? How can we enable Internet of Things ("IoT") innovation while addressing the full spectrum of risks associated with cyber-physical systems? How can a common understanding of security needs enable faster and more efficient adoption to improve security without sacrificing accountability?

The online industry is still young and growing and changing at an ever rapid pace. A light touch is the best way to approach most new threats and challenges. First, the market may adapt on its own. In addition, the nature of the threat or challenge may not be fully known, and any policy or reaction based on incomplete information is bound to create additional problems. On the other hand, what would be most helpful would be investment in new technologies, startup incubators, business models, and educational programs stressing engineering and computer science.

It is clear that law enforcement needs to evolve to meet the threat of malvertising, and cybersecurity in general. Technologies like drones and the IoT for example, are prone to abuse. While regulation of the technology itself would stifle innovation, updating of law enforcement sophistication and legal means to pursue true cybercriminals would actually foster a friendlier environment for business online. Keeping in mind the principles listed above, the i2Coalition suggests that efforts be made to educate and empower law enforcement to effectively respond to the threat of SPAM, malvertising, botnets, and other explicitly criminal methods of attack on legitimate businesses and individuals online, rather than attempt to insert backdoor decryption keys or other unsustainable quick-fixes. Further, law enforcement should specifically refrain from prosecuting marginal violations of laws where there is no significant harm, loss of property, privacy, or defamation, or where the violations are political in nature (e.g. promotion of free speech or the rights of the public to access online information). This will improve the perception of government efforts online in the public eye while simultaneously providing an improvement in the environment for businesses seeking to advance technology and create economic value.

INTERNET INFRASTRUCTURE COALITION



718 7th Street NW
2nd Floor
Washington DC 20001

staff@i2coalition.com
(202) 780-7237