



Via electronic email to cybertaskforce@doc.gov

September 20, 2010

Office of the Secretary
National Telecommunications and Information Administration
International Trade Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: Department of Commerce, Notice of Inquiry
Cybersecurity, Innovation and the Internet Economy
Docket No. 100721305-0305-01

The Online Trust Alliance (OTA) hereby submits its comments to the Department of Commerce's Notice of Inquiry, dated July 28, 2010.

Core to OTA's mission is the protection of users' online trust and confidence which we believe are the foundation for continued innovation and the vitality of the Internet economy. OTA is encouraged by the dialog between business, industry and government to help protect both the Nation's critical infrastructure and consumers. This requires a renewed focus, investment and willingness to change business practices as the onslaught of cybercrime and deceptive businesses continues to tarnish online trust, compromises users' identity and illegally obtain confidential business information.

While we have seen progress fighting spam, forged and spoofed email continues to plague leading financial institutions, commerce sites and government agencies. Email authentication is a proven remedy, yet based on a report OTA is publishing on September 24th ([Email Authentication Adoption Progress Report](#)), only 60 percent of the top 100 financial services companies, 42 percent of the Fortune 500, and 58 percent of the Internet Retail 500 are taking adequate steps to protect consumers and brands from deceptive email. Equally troubling is that only 40% of the top consumer facing U.S. government domains are authenticated their domains and outbound email servers. While email authentication is now included as a call to action in the draft National Strategy for Trusted Identities in Cyberspace (NSTIC), adoption needs to be accelerated to better protect citizens, business and Federal employees from online abuse and obtaining confidential and classified information.¹

¹ <https://otalliance.org/resources/authentication/index.html>

Cybercriminals have expanded their scope of impact focusing on trusted web sites and abusing the ad serving infrastructure. OTA research has revealed that in Q2 2010 malvertising increased 250%, with over 50 ad networks being found to be distributing compromised ads. In the absence of integrated controls, standards and end-to-end accountability, these intrusions are flourishing. Cybercriminals are increasingly exploiting weaknesses in the ad serving ecosystem, offering the ability to remain anonymous with expansive malware distribution capabilities. We believe stakeholders need to allocate resources to help counter this abuse. In early September OTA released draft anti-malvertising guidelines calling for public comments to address this emerging threat.² It is our goal to facilitate input with stakeholders and secure their commitment to adopt these voluntary guidelines to help protect consumers from this abuse. We look to the Commerce Department for support to accelerate efforts to help stem this quantifiable harm to consumers.

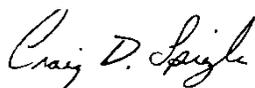
For background, OTA was founded in 2004 to address the global spam problem and the lack of standards to help detect forged email. In the past six years, OTA has grown significantly. As an IRS approved 501c6 member- based non-profit, we represent the broad Internet ecosystem and are not beholden to any special interest group. OTA is comprised of over 70 business, industry and technology leaders who share our mission to enhance online trust while promoting business practices and technologies which support the vitality of online services. <https://otalliance.org>.

This past twelve months has marked several OTA milestones including the publishing of:

- Proposed Data Collection & Privacy Statement https://otalliance.org/privacy_demo.html
- Online Principles & Business Guidelines <https://otalliance.org/resources/principles.html>
- Data Loss & Breach Readiness Guide <https://otalliance.org/resources/Incident.html>
- Online Safety Honor Roll https://otalliance.org/news/releases/2010honor_roll.html
- Submissions to the Privacy Act staff discussion draft from Representatives Boucher & Stearns https://otalliance.org/docs/OTA_Privacy%20Bill_finalx.pdf
- Submission to the "Best Practice Act" https://otalliance.org/docs/Rush_OTA_Privacy_8-23.pdf
- National Strategy for Secure Online Transactions (NSSOT)
- OTA Anti-Malvertising Task Force <https://otalliance.org/resources/malvertising.html>

Attached you will find a summary of responses to key questions cited within the NOI. OTA looks forward to continuing collaboration with the Department of Commerce. Working together we can help ensure the vitality of the Internet and commerce.

Respectfully,



Craig Spiegle
Executive Director
Online Trust Alliance

Cc: OTA Board of Directors & Steering Committee

² OTA Anti-Malvertising <https://otalliance.org/resources/malvertising.html>

In response to the Notice of Inquiry, the following reflects OTA's members input:

Quantifying the Economic Impact

The health and vitality of the U.S economy increasingly is reliant on reliable communications, information and trusted transactions. Trust and confidence are the foundation of commerce, requiring greater collaboration and information sharing between the public and private sectors. Within existing protected communities of trust, including Information Sharing and Analysis Centers and InfraGard, companies are voluntarily sharing information on threats, vulnerabilities, countermeasures, and best practices, to their mutual benefit. ISACs have matured to the point that they are regularly sharing both anonymized and attributable information between ISACs and with the Federal government and US-CERT. However, unrestricted sharing with government entities and the public is limited by a host of outside influences and concerns which often outweigh the benefits of doing so.

Similar to past experiences with spoofing, breaches and phishing fraud, individual brands (e.g. banks and commerce websites et al) harbor concerns about the impact of sharing information including; increasing consumer angst, negative impact to a brand's reputation, possible exposure to additional malicious activity, and consumer distrust of their legitimate web properties and interactive marketing initiatives. Additionally there is fear of a negative impact to shareholders value and the risk of conflating the issues, inviting regulatory intervention.

At a time when the industry most needs to come together to build upon these successful partnerships, some firms find themselves in the cross-hairs of regulatory enforcement for purported misuse of data collected in the course of their business operations. This is an area for potential governmental review, to provide guidance and processes to support expanded public-private information interchange, including enhanced definition of the types of data to be shared (forensic, metrics, etc.), limitation of information usage and potential economic incentives to ease the burden of regulatory compliance. Government should endorse and raise awareness of existing information-sharing architectures and encourage companies to voluntarily participate, rather than impose regulatory compliance and reporting.

Raising Awareness

Technology alone cannot counter all misuses of the Internet and connected networks and systems. User education and advice is required to reduce the number of at-risk of PCs and instill safe browsing practices. The need for education is not limited to consumers, but equally as important to business users and small businesses.

We applaud efforts such as the FTC's Oguard-Online campaign to help educate consumers to cyber security risks. At the same time we are concerned that too much reliance is being placed on broad-reach awareness initiatives. While continuing to support these efforts, OTA believes the Commerce Department should allocate equivalent if not greater resources and incentives, including support of pilot programs focusing on remedial or solution oriented teachable moments.

Consumers today interact with a wide range of online services, many of which include banking and ecommerce. These businesses can leverage their consumer facing sites by incorporating educational and prescriptive advice at point of data collection and user interaction. For example, during web sessions and user authentication, a bank or commerce site could detect an end-of-life browser or browser plug-in. A teachable moment might encourage the user to upgrade their browser, explaining the security and privacy benefits, and providing the respective link(s) to download updates.

Secondly, the Department could point business owners to resources produced by the private sector and NGO community. For example, OTA in collaboration with the US Chamber, Direct Marketing Association, Internet Security Alliance and the Anti-Phishing Working Group published a [Data Breach Incident Readiness Planning Guide](#) along with a broad range of other resources.³ Other organization and government agencies have made similar efforts, which are in need of support and funding. Examples include resource kits, train-the-trainer toolkits, marketing copy, and graphics, which can easily be branded for employee training and community based programs.

The NGO community along with private industry support is uniquely positioned to contribute to the composition and promotion of such teachable moments, without a bias of any direct business objectives or trade organization's agenda. Further, OTA recognizes that at-risk environments include not just consumer machines, but the long tail of small and medium-sized businesses that may not be trained, resourced, or equipped to adequately prevent these exploits.

Web Site and Component Security

As operating systems and browsers have become more secure, cyber criminals are increasingly targeting web sites, applications and browser plug-ins. Since 2005, the percent of virus-laden email reaching consumers have decreased 94%, while malware infected web pages have increased over 600%. OTA research has revealed that in Q2 2010 malvertising increased 250%, with over 50 ad networks being compromised. In the absence of integrated controls, standards, and end-to-end accountability, these intrusions are flourishing. While these exploits proliferate preying on at-risk PCs, site owners and infrastructure providers share the responsibility for securing their sites and business processes from these exploits. OTA has published a series of voluntary online principles and guidelines to help address these threats.⁴ Working with the Commerce Department, it is our hope that these guidelines will be rapidly deployed.

Authentication/Identity (ID) Management

Authentication and Identity management are critical components of a trusted cyberspace ecosystem. The draft of the White House's National Strategy for Trusted Identities in Cyberspace (NSTIC) offers the potential for enhanced privacy and security, helping to address the risks of password mismanagement, including phishing and identity theft. Consumers today typically use a limited set of passwords (sometimes just one) as their primary credentials to login to sites. Directionally the NSTIC is a sound strategy to help balance identity and password management with security and privacy concerns. NSTIC will take time to implement, but many of the underlying technologies and practices can be deployed today.

For the past 5 years OTA has been advocating best practices in three areas; 1) Email authentication to counter email forgers, 2) Extended Validation SSL Certificates to add an additional layer of identity to the sites a consumer visits, and 3) more effective password management.

³ <https://otalliance.org/resources/Incident.html>

⁴ <https://otalliance.org/resources/malvertising.html>

1. Email Authentication builds on existing IETF standards (e.g. DKIM, SPF, and ADSP) to validate the sender of the email. Not only does this help protect the user from malicious email, it also aids in the protection of a business's reputation from abuse and forgery, and the financial costs from malicious emails result in account takeovers, system damage, data loss and/or identity theft.⁵
2. Extended Validation SSL Certificates - EV SSL Certificates are deployed by over 30,000 commerce and banking sites were created to address the rise in Internet fraud that was eroding consumer confidence in online transactions. EV SSL certificates help verify a Web site owner through a comprehensive validation process. When consumers visit a site with an EV SSL certificate, the address bar turns green, representing a trust indicator. In addition a user can click on the company name for more intuitive data including where the company is located and incorporated. The rapid development of EV SSL is credited to the work of the CA/Browser Forum and the work of leading Certificate Authorities and browser vendors.
3. Passwords – User passwords are often overlooked and by themselves can be easily exploited. Frequently cited reasons include: use of common names can often be easily discovered by visiting a Facebook or LinkedIn page, infrequent changing of passwords, allowing for re-use of past passwords, and ineffective security challenge response questions used to re-set passwords. OTA has published recommendations to aid in creating such challenge questions, balancing security and usability. OTA suggests the following criteria be considered in the structure of any such questions and allowable answers; 1) answer pool size, 2) variability of the answer, 3) public information, 4) common compromise information, 5) social engineering susceptibility, 6) answer commonality, 7) applicability, 8) memorability, and 9) repeatability or ability for a user to remember.⁶

Research and Development

Innovation has been a keystone of the American economy. Public-sector investment in cybersecurity research is critical, but must work in concert with the private sector. The Cybersecurity and Information Assurance Interagency Working Group (CSIA IWG) under the National IT Research and Development (NITRD) program focuses and prioritizes Federal R&D investment, including “Leap Ahead” projects. We support increased funding for this program, and encourage continued collaboration with the private sector. Today there is a gap between research, which is often focused on strategic game-changing large-scale solutions, and best practice development and deployment. We believe there is an opportunity to take conceptual and theoretical work and actively drive pilot programs, rapid prototyping, and spur early adoption and deployment. This can be accomplished by dedicating budgetary funds and project management resources.

The scope of public and private investment should not be limited solely to large multinational organizations. Small business innovators are often not equipped to meet application submission requirements. By streamlining processes and creating a “fast-track” application and reporting processes (similar to the 1040EZ IRS tax return form), emerging businesses would be able to increase their contribution leveraging their high level of innovation, agility and ability to bring concepts to market. Doing so fosters an opportunity to cost effectively accelerate the development of technologies and solutions and proof of concept testing.

⁵<https://otalliance.org/resources/authentication/index.html>

⁶<https://otalliance.org/resources/index.html>

An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

Businesses already have strong incentives to protect their assets, including intellectual and physical property, customer relationships and data, their brand, and supply chains. These incentives vary widely, based on differences in products, geography, value chains, and other factors. Therefore, OTA recommends the focus be on motivating good behavior through an incentives-based business model defined by a dynamic risk management approach. OTA supports such an approach, versus regulations which risk encumbering innovation. Self-management and monitoring is recommended, focused on providing incentives for the private sector to push forward with public and private sector endorsed identity management goals and best practices. Efforts and resources need to be allocated to recognize and incentivize organizations' efforts in three key areas: 1) development and implementation of best practices; 2) tracking, measurement and reporting of adoption; and 3) providing recognition to early adopters.

Government can positively impact business security investments by sharing timely, specific, and actionable threat intelligence. This can include information and data sharing regarding the cascading effects of incidents that could have national or critical infrastructure impact. As business owners and operators become aware of threats to their businesses or customers, or of national interest, they will act to protect their own interests. Likewise, providing recognition of a company's efforts should be highlighted as "north stars" for others to follow. In this regard, OTA directly supports an annual awards program for individuals, businesses, and NGOs who demonstrate excellence in these categories, including best practices, innovation, information sharing and collaboration.⁷ The 2010 awards announced on September 23, include categories in individual leadership, organizations and businesses for their commitment to the protection of consumers and critical infrastructure.⁸

⁷ <https://otalliance.org/resources/initiatives.html>

⁸ <https://otalliance.org/news/releases/2010awards.html>