OTA
Online Trust Alliance

August 1, 2011

Send via email to SecurityGreenPaper@nist.gov

Mr. Patrick Gallagher,
Under Secretary of Commerce for Standards and Technology
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue N.W.
Room 4725
Washington, D.C. 20230

RE: Comments on Cybersecurity Innovation & The Internet Economy Green Paper
Docket No. 110527305-1303-02

Dear Mr. Gallagher,

Thank you for providing the Online Trust Alliance, (OTA), the opportunity to submit comments on the Cybersecurity Green Paper. As a member-based non-profit, OTA includes over 85 organizations representing the internet ecosystem. OTA's mission is to develop and advocate best practices and public policy to mitigate privacy, identity, and security threats to online services, brands, organizations and consumers, thereby enhancing online trust and confidence.

As echoed in the Green Paper, OTA believes privacy and security are key risks directly impacting online trust and confidence and the economic stability of our nation. The importance of preserving and in some cases regaining trust cannot be overstated. Businesses of all sizes and across all sectors rely on the willingness of consumers and organizations to entrust them with their information. This reliance assumes that their information will be used, shared and stored as agreed, aligned to their expectations, and that all parties will take steps and precautions to protect their data from abuse and loss. OTA believes these expectations are a foundation principle for commerce and the global internet economy and needs to become standard operating procedures for all entities. Without this assurance and data stewardship, we risk a "trust meltdown".

A second essential trust principle is the commitment to multi-stakeholder policymaking, standard development and creation of voluntary codes of conduct and adoption of best practices. Solutions must work across the ecosystem and address the long-term impact and risks, while supporting innovation in online services. It is OTA's aspirational goal that security and privacy become brand and product differentiators, becoming part of the value proposition offered to consumers and business alike.

OTA has a long-history of supporting such efforts and codes of conduct including ISP best practices, as well as publishing specific guidelines for countering malvertising, driving adoption of email authentication, enhancing security of email service providers and publishing data breach readiness guidelines.[1, 2, 3, 4] OTA believes that our economy is best suited with the adoption of voluntary code of conducts over added legislation and regulations, which an encumber legitimate businesses and stifle innovation. This position is based on the assumption that such guidelines are not self-serving and are meaningful, actionable, and measurable. Today in the absence of such measures, we are seeing consumers and advocacy group demand regulatory intervention in several areas. Industry and business would be well served if NIST could aid in increasing awareness, promoting existing standards and practices from the NGO community, and assisting in the development of new ones where gaps exist.

OTA supports many of the key standards as outlined in the Green Paper, and provides the following additional perspectives and clarification.

User Education & Teachable Moments - While broad based education campaigns such as Stop, Think, Connect are important, OTA believes that we can increase cybersecurity and reduce online fraud, account takeover and identity theft though “teachable moments”. Teachable moments are defined as educational opportunities at time of user interaction with a site they visit or online service they frequent. Rather than solely relying on a user seeing an advertisement and taking action, the same message should come from a site that a user has made a decision to visit and / or has a trusted relationship with.

For example, while the merits of updating a user’s browser with the latest security and privacy capabilities are well known, only a handful of sites inform the users at login or at time of a transaction. Leading browsers have integrated phishing, malware detection and URL reputation analysis, as well as enhanced privacy features including support of the “Do Not Track Header” and related privacy controls. It is proposed sites analyze the “user string” of the client accessing their service. When a user attempts to log into the bank, the site could recognize that the user has an out of date browser and suggest an upgrade, with a link to a page outlining the importance and steps for upgrading.[5]

[1] Anti-Malvertising Guidelines - https://otalliance.org/resources/malvertising.html

[2] Security by Design Email Marketing Guidelines - https://otalliance.org/resources/securitybydesign.html

[3] Data Incident Planning Guide - https://otalliance.org/resources/Incident.html

[4] Email Authentication https://otalliance.org/resources/authentication/index.html

[5] Consumer facing information will address use cases why upgrades need to be considering compatibility of enterprise line of business application or users with end-of-life operating systems.

Recognizing the importance of such efforts, OTA is soliciting collaboration with NIST, DHS, NGOs and all browser vendors to promote browser upgrades this October as part of the National Cybersecurity Month. OTA is proposing the creation of a tool kit including graphics, copy and code for sites to incorporate within their sites, including consumer facing narrative on the security and privacy value proposition of upgrading. As recent security and privacy innovation has been a priority with most leading browsers, this is an opportunity to educate consumers and harden the first line of defense.

Name Security (DNSSEC) – DNSSEC is an OTA best practice, supported by US Government policy since the 2003 and now a component of the National Strategy to Secure Cyberspace.[6] NIST could aid in the deployment of DNSEC by individual domains by both measuring and reporting on adoption by key stakeholders, including ISPs, financial institutions, ecommerce websites, and other sites with which public trust is a critical factor. DNSSEC is essential in ensuring trust on the Internet through blocking, for example, man in the middle attacks that are central to phishing. Towards this goal, tools need to be developed to support the small to medium business segments that typically run their sites on virtual or shared hosting environments. With roots having been signed for the three major gTLDs, .org, .com, and .net, OTA is planning on expanding tracking adoption across multiple sectors this fall. [7]

Web Security – "Always on" SSL is highly recommended for all banking, commercial, and social networking sites, as well as web-based messaging platforms. While it is common for websites to protect passwords by encrypting the initial login, few websites encrypt everything else. HTTP session hijacking (also called "sidejacking") occurs when an attacker gets hold of a user's cookie, allowing the interceptor to do anything that the user can do on a particular website. This can be accomplished by downloading simple tools such as Firesheep, or setting up "free" wireless access points or evil twins and sniffing internet traffic.[8, 9] The solution is the use of TLS/SSL site-wide, offering full end-to-end encryption known on as HTTPS or SSL. Early adopters in this effort include Bank of America, Twitter, PayPal, Google Gmail, the Online Trust Alliance (OTA), and other leading sites who have recognized that the impact to CPU utilization is minor and predictable in the overall scope of operations and security and privacy benefits to the user.

[6] http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

[7] May 2011 Online Trust Scorecard - https://otalliance.org/news/releases/2011scorecard.html

[8] Firesheep is an extension for Firebox released in October 2010. It uses a packet sniffer to intercept unsecured cookies. It captures the names of user on the local network and the services they are connected. http://codebutler.com/firesheep

[9] Evil twin is a term which refers to the use of setting up wireless hotspots offering free access deceptively using names associational with local businesses in an effort to collect user data and / or log on credentials.

Email Security – Adoption of email authentication has been a key initiative of OTA since 2004. While email authentication does not in itself reduce spam or increase security of email messages, it offers the ability of receiving networks to detect and block spoofed and forged email. The most effective approach is the combination of both SPF and DKIM together. The need for inbound and outbound authentication has been highlighted by the increased precision or personalization of spear and whale phishing, targeting business users and government employees. As email continues to be the attack vector of choice, all domain holders should be authenticating all of their outbound mail streams and incorporating inbound validation. OTA provides training and resources to aid ISPs, businesses, and government agencies in the deployment and management of email authentication.[10] [11]

These comments reflect the general consensus of our membership and technical committees. On behalf of OTA, we look forward to working with the Department of Commerce and other stakeholders to help increase online trust and confidence while enhancing innovation and the vitality of the internet.

Sincerely,

Craig D. Spiezle

Executive Director and President
Online Trust Alliance
Craigs@otalliance.org

[10] Email Authentication Resources https://otalliance.org/resources/authentication/index.html
[11] Email Authentication Training https://otalliance.org/events/2011_Forum/Academy.html#1_Email_Authentication_Training