



May 27, 2015

Mr. Allan Friedman
National Telecommunications and Information Administration
U.S. Department of Commerce, 1401
Constitution Avenue NW., Room 4725,
Attn: Cybersecurity RFC 201,
Washington, DC 20230.

securityRFC2015@ntia.doc.gov

RE: Request for Public Comment Stakeholder Engagement on Cybersecurity in the Digital Ecosystem
Docket No. 150312253–5253–01 / RIN 0660–XC018

Dear Mr. Friedman,

Thank you for providing the Online Trust Alliance (OTA) the opportunity to respond to NTIA's request for comments regarding multi-stakeholder cybersecurity best practices. As a 501c3 non-profit organization, OTA's mission is to enhance online trust and empower users while promoting innovation and the vitality of the Internet. OTA works to educate businesses, policy makers and stakeholders about best practices and tools that enhance the protection of users' security, privacy and identity.¹

OTA prides itself as an active and objective participant in multi-stakeholder initiatives from fighting spam and botnets, to addressing domain collision issues and advancing mobile security, facial recognition and privacy enhancing best practices. These include participation in past NTIA efforts and the Federal Communications Commission's Communications Security, Reliability and Interoperability Council, (CSRIC).²

Collectively we believe multi-stakeholder efforts must be open, transparent and develop consensus by providing an equitable and fair opportunity for interested parties to participate. Processes need to be established to help keep discussions, priorities and scope from being dominated by special interest and dominate market players. We believe a facilitated led process will effectively drive the formation of best practices to allow us to improve the security, stability and resiliency of Internet. It is important to note that as the stakeholders are typically geographically diverse, meetings need to accommodate those in different time zones and promote remote participation. In addition the cost, benefits and incentives for

¹ <https://otalliance.org/about-us>

² FCC CSRIC <http://transition.fcc.gov/pshs/advisory/csrc/>

cyber security must also be addressed and considered when developing best practices and any self-regulatory models.

Where possible NTIA should leverage related efforts including those driven by National Institute of Standards and Technology (NIST), the FCC CSRIC, Federal Trade Commission and Department of Homeland Security. It is important to recognize that some of the practices and controls outlined in these efforts while being applicable to critical infrastructure may not be applicable or cost effective to the broader group of stakeholders. Conversely some of the specific areas listed in the RFC such as malvertising may not have been a top priority for the NIST framework or by ISPs with the FCC's CSRIC, yet may be better suited for a broader multi-stakeholder effort as proposed by NTIA.

As data sharing is key to help detect and prevent exploits, Commerce should consider adopting information sharing models created by the Department of Homeland Security including Structured Threat Information Expression (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII).^{3,4} Such models facilitate the collection and offer the promise of timely dissemination of threat intelligence.

OTA supports public recognition of companies who have demonstrated leadership in security and privacy. For the last seven years OTA has completed an independent audit of nearly 1,000 web sites assessing security and privacy enhancing best practices. Organizations who make a threshold on adoption of best practice are named to the Online Trust Honor Roll recognizing their respective leadership.⁵ Such affirmation should be considered to encourage the adoption of best practices.

The following is a summary key areas OTA recommends for inclusion in multi-stakeholder review.

a) Botnet Mitigation

Botnets pose one of the biggest threats to Internet security and present an opportunity for an actionable and collective progress. Collaboration and data sharing need to be accomplished across multiple stakeholders. It is important to leverage the work of FCC CSRIC, and the resulting Anti-Bot Code of Conduct for ISPs. It is recognized the problem is much boarder and requires participation by the hosting community, web authoring and content management platforms and related infrastructure providers. Working to broaden participants, OTA convened a working group including the hosting community, AV vendors, financial institutions and others resulting in the publication of Botnet Remediation Best Practices white paper. This effort developed a framework for the anti-botnet lifecycle (prevention, detection, notification, remediation and recovery) addressing a number of key best practices including connecting user notification with remediation tools, preventative measures, and related efforts.⁶ This effort needs added engagement and support to help accelerate the adoption of anti-bot best practices and are well suited to a multi-stakeholder effort.

³ <http://stix.mitre.org/>

⁴ <http://taxii.mitre.org/>

⁵ Online Trust Audit & Honor Roll <https://otalliance.org/HonorRoll>

⁶ https://www.otalliance.org/system/files/files/best-practices/documents/ota_2013_botnet_remediation_best_practices.pdf

b) Trust in and Security in Core Internet Infrastructure: Naming, Routing, and Public Key Infrastructure Domain Name System (DNS), Border Gateway Protocol (BGP), and Transport Layer Security (TLS) Certificates

The Domain Name System (DNS) enables nearly all Internet transactions today. Its operation and inherent systemic dependencies are critical yet commonly overlooked when calculating an organization's attack surface and conducting risk management and mitigation activities. Understanding the implications of the DNS control plane and the full benefits of DNS Security Extensions (DNSSEC) can help to minimize your attack surface and enhance your security posture. In the US, measurements suggest that approximately 25% of end-users have access to DNSSEC validation support, largely due to several very large stakeholders support.⁷ Unfortunately adoption with the exception of US. Government sites remains in the single digits.⁸

Key aspects of the Internet infrastructure have long been known to be vulnerable. Enhancing the stakeholder discussions in these areas should lead to new cyber security capabilities and drive adoption of others. For example, mail service providers have actively taken up DNSSEC and DNS-based Authentication of Named Entities (DANE) to afford scalable means for discovering certificates that allow TLS connections between them. This benefits the digital ecosystem because it adds a security methodology for enterprises that might fear giving opportunities to malicious entities that access their email streams in clear-text passing from one enterprise to the other. The multi-stakeholder effort could help increased awareness and the value proposition of several such solutions including, DNSSEC, DANE and certificate transparency (CT) to help make the infrastructure more resilient and trustworthy.^{9 10}

c) Web Security

Many consumers assume that their connections with websites are secure, and that the websites they conduct banking, commerce and communications have adopted such safeguards. OTA believes this is a key area where we can realize results in the short-term to address not only the technical issues, but the ongoing operational issues which are leaving sites vulnerable. OTA's audits of leading sites year-after-year reveals gaping holes in SSL security. While many of these vulnerabilities can be fixed in minutes, more often they remain undetected and unpatched. OTA strongly encourages the deployment of HSTS or Always On SSL, (AOSSL), encrypting the entire web session between the user's device and website.¹¹ AOSSL not only enhances user security, but equally as important the help protect the privacy of their online activities from third parties. Recently leading government sites include the Federal Trade Commission and the White House have adopted AOSSL.^{12, 13}

⁷ <http://gronggrong.rand.apnic.net/cgi-bin/worldmap>

⁸ See 2015 Online Trust Audit <https://otalliance.org/HonorRoll>

⁹ <https://otalliance.org/resources/dnssec>

¹⁰ http://blogs.verisigninc.com/blog/entry/what_s_in_a_name

¹¹ <https://otalliance.org/AOSSL>

¹² FTC <https://www.ftc.gov>

¹³ <https://www.whitehouse.gov/>

d) **Malvertising**

Criminals have recognized the interactive ad ecosystem is fertile groups for abuse. The frequency of malicious advertising insertions continues to grow with increased precision and payload capabilities, resulting in over 10 billion malicious ad impressions in 2014.¹⁴ Unfortunately adoption of best practices which could greatly diminish the effectiveness of this threat have been rebuked by leading trade groups and dominate market players. Adding to the complexity is the broad number of stakeholders and intermediaries including advertisers, ad networks, ad exchanges and others and the increased reliance on automated programmatic ad buying.

Working together, these parties can establish best practices and implement circuit breakers to help decrease the effectiveness of malvertising. While the advertising community has made progress to limit click fraud which impacts the economics of advertising, efforts to stem the harm from malicious has been limited as identified by the U.S. Senate Permanent subcommittee on Investigation (PSI), in May 2014.¹⁵ To-date the best practices to help protect infrastructure has been to block all third party content and ads, block users from sites which serve ads and sandbox applications and devices. OTA believe malvertising should be a top priority for the task force.

e) **Internet of Things (IoT)**

As consumers and businesses acquire IoT devices, there is an amplified security and privacy risk with every additional device connected to the user's personal and business network. While many of these short comings have since been addressed by leading websites and mobile app developers, disappointingly many IoT vendors have yet to follow or learn from their mistakes. In Symantec's report analyzing IoT devices for vulnerabilities, wide spread security concerns were discovered.¹⁶ Further data suggests widespread location tracking is occurring without consumer notice and or consent.¹⁷ As reported by the National Security Telecommunications Advisory Committee's report to the President, it determined that there is a small and rapidly closing window to ensure that IoT standards and practices are adopted in a way that maximizes security and minimizes risk." The report concluded "If the country fails to do so, it will be coping with the consequences for generations^{18, 19}

OTA's independent research completed in late May 2015 revealed 14% of leading IoT devices lack privacy policies and others fail to encrypt any personal data between the device, the application and the cloud.²⁰ In an effort to help these concerns OTA has stood up a multi-stakeholder working group to help develop a trust framework address key security, privacy and sustainability issues and best practices.²¹

¹⁴ <https://otalliance.org/resources/advertising-integrity-fraud>

¹⁵ <http://www.hsgac.senate.gov/hearings/online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy>

¹⁶ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf

¹⁷ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf

¹⁸ <http://www.pcmag.com/article2/0,2817,2482620,00.asp>

¹⁹ <http://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf> - November 2014

²⁰ See June 2015 Honor Roll report <https://otalliance.org/HonorRoll>

²¹ <https://otalliance.org/IoT>

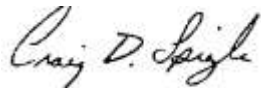
f) **Privacy**

As noted in the Cybersecurity Framework, privacy and civil liberties implications arise when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities. OTA recommends addressing privacy in the multi-stakeholder process, though perhaps as a component of every security issue being addresses by the multi-stakeholder process. Working cross stakeholders and privacy advocates, will enable the formulation of best practices on sanitizing data before sharing or when receiving information. Additionally, best practices can be developed around agreements to keep threat data confidential when shared and how to address the eventual leakage of personal information when shared for security purposes. OTA recommends the scope of the multi-stakeholder effort include both consumer and business data.

In summary, OTA looks forward to participating in multi-stakeholder efforts which facilitate collaboration leading towards the development of best practices. Equally as import is the establishment of incentives for businesses including providing positive affirmation and safe harbor provisions.

Thank you in advance for your efforts to help improve the security and resiliency of the internet.

Sincerely,



Craig D. Spiegle
Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
<https://otalliance.org>
+1 425-455-7400