

May 24, 2016

National Institute of Standards and Technology  
Attn: Computer Security Division, Information Technology Laboratory  
100 Bureau Drive (Mail Stop 8930)  
Gaithersburg, MD 20899-8930

**RE: Comments of ACT | The App Association regarding *National Institute of Standards and Technology Special Publication 800-150, Guide to Cyber Threat Information Sharing (Second Draft)* (Docket No. FDA-2015-D-5105)**

ACT | The App Association writes to provide input to the National Institute of Standards and Technology (NIST) on its second draft Special Publication 800-150, Guide to Cyber Threat Information Sharing.<sup>1</sup>

ACT | The App Association represents more than 5,000 app companies and technology firms that create the apps used on mobile devices around the globe. As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions across modalities and segments of the economy. Across these segments, niches, and communities, organizations benefit from the enhanced ability to identify, assess, monitor, and respond to cybersecurity threats. We applaud NIST's efforts to provide guidelines for establishing and participating in cyber threat information sharing relationships. As we detail in our annually-released *State of the App Economy Report*,<sup>2</sup> while the app industry has been in existence less than a decade, it has experienced explosive growth alongside the rise of smartphones and has revolutionized the software industry, touching every sector of the economy.

The voluntary timely sharing of cybersecurity threat indicators among organizations from both the public and private sector will be crucial in the detection, mitigation, and recovery of cybersecurity threats, particularly with the rise of the Internet of Things (IoT). We applaud NIST's draft for including discussion that captures the wide scope of organizations, from the most formal to the least, which can be of assistance to organizations looking to improve their cybersecurity posture through the sharing of threat information. For example, Information

---

<sup>1</sup> NIST, *SP 800-150, DRAFT Guide to Cyber Threat Information Sharing (Second Draft)* (Apr. 21, 2016), available at [http://csrc.nist.gov/publications/drafts/800-150/sp800\\_150\\_second\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf).

<sup>2</sup> ACT | The App Association, *State of the App Economy 2016* (Jan. 2016), available at <http://actonline.org/state-of-the-app-economy-2016/>.

Sharing Analysis Organizations (ISAOs), which are envisioned in Executive Order 13691<sup>3</sup> to be formed to fill needs for unique communities, large and small, sometimes across economic segments. ISAOs, as a complement to Information Sharing Analysis Centers (ISACs), are expected to help to address the resource limitations of small businesses as well as the convergence of business models that may make it difficult to determine the best way to engage in information sharing. ACT | The App Association encourages NIST to ensure that these key fora are included in its guidance to federal agencies and stakeholders at large.

Further, for small businesses like ACT | The App Association's members which are increasingly threatened by cyber-based attacks, where and how to allocate limited resources is a significant challenge to information sharing. Other key NIST efforts, such as the NIST Cybersecurity Framework<sup>4</sup> (and others influenced by NIST's approach) have embraced a scalable cybersecurity risk management approach generally which lends to a feasible approach by these smaller entities. As the digital economy continues to expand, powered by smaller organizations that develop software apps, fluid bi-directional sharing of information between and among these entities and the government will be crucial.

Based on the above, ACT | The App Association urges NIST to incorporate the changes and recommendations included in our appended Comment Template Form. ACT | The App Association appreciates the opportunity to provide input to NIST in this matter and stands ready to work with NIST on this and related efforts.

Sincerely,



Morgan Reed  
Executive Director  
ACT | The App Association

---

<sup>3</sup> Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (Feb. 13, 2015), <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.

<sup>4</sup> NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014), available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change
1	ACT   The App Association	ACT   The App Association	Substantive	5	358	2.1	Information Sharing and Analysis Organizations (ISAOs) should be included in NIST's list of potential sources of Security Alerts.	after "...(ISACs)," insert "Information Sharing and Analysis Organizations (ISAOs),"
2	ACT   The App Association	ACT   The App Association	Substantive	7-8	427-480	2.3	Particular for small businesses which are increasingly threatened by cyber-based attacks as the digital economy proliferates, where and how to allocate limited resources is a significant challenge to information sharing. This Special Publication should address this very real and widely-acknowledged barrier.	ACT   The App Association suggests that NIST include the following text as a new bullet (where appropriate within Section 2.3): " <b>Organizational Use and Distribution of Resources.</b> Organizations, based on their characteristics and circumstances, will face important decisions around how to allocate resources towards developing processes to share cybersecurity threat information with other organizations. These resource constraints present unique challenges to any organization facing cyber-based threats to their operations."
3	ACT   The App Association	ACT   The App Association	Substantive	19	722	3.5	ISAOs will also become a key "sharing partner", and should be mentioned here.	after "...ISACs," insert "ISAOs,"

4	ACT   The App Association	ACT   The App Association	Substantive	29-31	1039-1159	Appendix A	<p>Given the rise of the mobile app economy which is powered by small businesses, ACT   The App Association encourages NIST to include a Scenario that addresses a small tech firm.</p>	<p>ACT   The App Association encourages NIST to consider developing a Scenario that would reflect a typical situation for a small business that would benefit from enhanced timely information sharing. We defer to NIST experts on where to include it within Appendix A, and on the specifics of the hypothetical save that it reflect the reality that a small business may need to utilize a holistic risk management approach to determine the best way for the entity to maximize the investment of its resources in information sharing fora.</p>
---	---------------------------	---------------------------	-------------	-------	-----------	------------	---	--