December 15, 2015

Speaker Paul Ryan  Democratic Leader Nancy Pelosi
United States House of Representatives  United States House of Representatives

Majority Leader Mitch McConnell  Minority Leader Harry Reid
United States Senate  United States Senate

Dear Speaker Ryan, Democratic Leader Pelosi, Majority Leader McConnell, and Minority Leader Reid,

The media associations in the Sunshine in Government Initiative (identified below) oppose a reported change to cybersecurity legislation that would effectively prevent access to any analysis or assessments of cybersecurity threats — whether classified or not — by state and local governments. These changes, which we understand to be drafted by the House and Senate intelligence committees and submitted to the conference committee almost entirely in secret, are not the way legislation should be enacted and could actually endanger our nation’s infrastructure by impeding government and public oversight of responses to cybersecurity threats.

Unfortunately, we have not seen a draft of the legislation. However, it is our understanding that two words would be added to the exemption from disclosure already included in cybersecurity legislation that has already passed both the House and Senate:

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared by or with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

The news media understand that private companies must be able to share certain information about cybersecurity threats with the government without fear of creating or increasing the danger of a cyber-threat. But the federal Freedom of Information Act (FOIA) already exempts from disclosure
information that would impede law enforcement investigations where a cyber-threat has occurred or would otherwise threaten personal privacy or national security or expose trade secrets.

While incremental changes might be needed to protect cybersecurity, this proposed two-word change is too broad and entirely unnecessary. At the same time it will prevent the public’s ability to protect itself. Correspondence, analyses, warning letters and general expressions of concerns generated by governments to private entities would not be disclosed to the public. So, a state or local government analysis on the readiness of an industry or areas of concern – even one written in general terms without revealing ways of defeating cybersecurity protections – would be exempt from FOIA. But these are exactly the types of reports the public should see. In the vein of “if you see something, say something,” this bill, applied to cybersecurity, tells the public, “if you see anything, ignore it because you shouldn’t have seen it anyway; we’ll tell you when to be concerned.” That is no way to defend against cybersecurity threats. Nor has such a wide-ranging exemption been necessary to date; for instance, similar general reports drafted by Government Accountability Office are routinely made available but have never led to an instance of harm.

What is more likely to happen is that incomplete or inaccurate reporting will compound a cyber-threat or curtail the government’s and public’s joint efforts to respond. Independent experts in this country and abroad are often the first to publicly assess malware or other cyber threats. Much of the conversation about cybersecurity threats occur in public and are reported on by media. This legislation would fuel misinformation. It would also hinder responses to inaccurate statements, as government officials elected by and held accountable by the public would be unable to make public statements without violating this provision, even after an attack or incident with large-scale consequences.

The public has an enormous stake in cybersecurity, including the privacy of consumer information; the cost of cybersecurity threats to banking, retail and insurance markets; and government actions to address this threat to our nation’s interests. Any proposal to curtail accurate news reporting to inform the public should, at a minimum, be publicly debated. That has not happened and it is a big mistake, as this two-word change could vastly curtail accurate news reporting about cybersecurity efforts and the response to cybersecurity threats.

We ask that you reject the two-word proposed change and work in public toward legislation that will incorporate public participation into our nation’s cybersecurity efforts.

Sincerely,

Rick Blum, Director