THE ASPEN INSTITUTE
HOMELAND SECURITY GROUP

Statement by Members of the Aspen Institute Homeland Security Group on the Cybersecurity Information Sharing Act of 2015

October 26, 2015

Members of the Aspen Institute Homeland Security Group, a bipartisan group of former national security officials and non-government policy experts, strongly urges the Senate to pass cybersecurity information sharing legislation along the lines of S. 754, the Cybersecurity Information Sharing Act of 2015 ("CISA"), now pending on the Senate floor.

Nearly every day we read of another serious cybersecurity breach at one major corporation and/or government agency or another. Simply put, our nation's most precious intellectual property and our most sensitive security information is not just vulnerable to theft, sabotage, or some other kind of compromise; it *is* being stolen, sabotaged, or otherwise compromised, on an ongoing basis and on a massive scale. This is a national security threat of the first order, and it is past time to do something about it.

A key part of the problem is that businesses are understandably reluctant to share information about cyber vulnerabilities, threats, and breaches with the government (and each other) out of fear that doing so will subject them to legal liability for the violation of their customers' and other private citizens' privacy rights and civil liberties. If the government is to help businesses mitigate cyber threats by addressing their vulnerabilities, and if the government is to help businesses respond to cyber attacks, it must have appropriate information regarding threats and vulnerabilities, and in as close to real time as possible.

Ideal information sharing legislation would incentivize information sharing with the government through the provision of liability protection and would ensure that such threat information is viewed in two perspectives. Information needed to protect the nation should be shared with all relevant agencies in the government at network speed, providing key agencies with the ability to act to accomplish their mission. At the same time, cyber threat information shared with the government for forensics purposes can and should be processed through a portal provided by the Department of Homeland Security ("DHS"). DHS is equipped to ensure that existing privacy and civil liberties protections are enhanced by scrubbing such forensic information before it is further disseminated and, as a civilian agency, can garner critical public support for such efforts.

Passage of legislation that incentivizes private sector entities to share cyber information with the government and each other, and, at the same time, that protects citizens' privacy rights and their civil liberties, is critical to the security of the nation. The Congress appears to be closer than ever before to making this a reality. Mindful that the perfect must not be the enemy of the good, we urge members to work out any remaining differences in pursuit of this vital goal.

Signed,

Charles Allen
Stewart Baker
Michael Chertoff
Philip J. Crowley
Michael Hayden
David Heyman
Clark Ervin
Juliette Kayyem
James Loy
Paul McHale
John McLaughlin
Michael Morell
Matthew Olsen
Eric Olson
Guy Swan