EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

April 21, 2015
(House Rules)

STATEMENT OF ADMINISTRATION POLICY

H.R. 1731 - National Cybersecurity Protection Advancement Act of 2015

(Rep. McCaul, R-Texas, and Rep. Ratcliffe, R-Texas)

An important building block for improving the Nation's cybersecurity is ensuring that private entities can collaborate to share timely cyber threat information with each other and the Federal Government. In January, the President submitted an updated legislative proposal to the Congress with the goal of, among other things, facilitating greater information sharing amongst the private sector and with the Federal Government. The Administration's proposal provides a focused approach to facilitate more cybersecurity information sharing while ensuring the protection of individuals' privacy and civil liberties. As the Administration has previously stated, information sharing legislation must carefully safeguard privacy and civil liberties, preserve the long-standing respective roles and missions of civilian and intelligence agencies, and provide for appropriate sharing with targeted liability protections.

The Administration commends the House Homeland Security Committee for its efforts to craft cybersecurity information sharing legislation with strong privacy protections. While the Administration supports House passage of H.R. 1731, improvements to the bill are needed to ensure that its liability protections are appropriately targeted to encourage responsible cybersecurity practices. The Administration recognizes the importance of the House and Senate working together to achieve these shared goals and supports advancing this legislation so that improvements can be made as the legislative process continues.

While the bill has improved significantly, the Administration still has concerns with H.R. 1731's sweeping liability protections. Appropriate liability protections should incentivize good cybersecurity practices and should not grant immunity to a private company for failing to act on information it receives about the security of its networks. Such a provision would remove incentives for companies to protect their customers' personal information and may weaken cybersecurity writ large. The Administration believes that a reasonable solution that strikes an appropriate balance can be found.

The Administration appreciates that the bill preserves the long-standing, respective roles and missions of civilian and intelligence agencies. Similar to the Administration's proposal, H.R. 1731 authorizes cybersecurity information sharing with a civilian agency, specifically the Department of Homeland Security's National Cybersecurity and Communications Integration Center. This approach will help protect privacy and provide appropriate transparency. In addition, charging one agency with facilitating the near real-time exchange of cyber threat indicators will enhance the efficacy of information sharing efforts and is more effective from an operational standpoint.

Cybersecurity requires a whole-of-government approach, including the ability to share relevant cybersecurity information quickly amongst relevant agencies. Once information is shared with the Federal Government, it should be shared with appropriate agencies in as close to real-time as

possible so that the Federal Government can use the information to better defend the Nation's networks. This sharing must be governed by certain narrow use limitations – an essential part of overlapping privacy and civil liberties protections that also rely on transparent oversight. The Administration would seek to clarify that information shared with the Federal Government can be used for investigating, prosecuting, disrupting, or otherwise responding to appropriate crimes.

H.R. 1731 also authorizes the use of certain potentially disruptive defensive measures in response to network incidents, provisions that were not included in the Administration's proposal. The use of defensive measures without appropriate safeguards raises significant legal, policy, and diplomatic concerns and can have a direct deleterious impact on information systems and undermine cybersecurity. Moreover, as drafted, these provisions may prevent the application of other laws such as the Computer Fraud and Abuse Act and State common law tort remedies. Though the Administration remains concerned that the bill's authorization to operate defensive measures is not adequately tailored, it is committed to working with stakeholders to address its remaining concerns.

Information sharing is one piece of a larger suite of legislation needed to provide the private sector, the Federal Government, and law enforcement with the necessary tools to combat cyber threats. In addition to updating information sharing statutes, the Congress should incorporate privacy and civil liberties safeguards into all aspects of cybersecurity and enact legislation that creates a strong and consistent notification standard for breaches of personal data, as well as legislation that gives law enforcement the tools to fight cybercrime in the digital age.

* * * * * * *