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

April 16, 2013
(House Rules)

STATEMENT OF ADMINISTRATION POLICY

H.R. 624 – Cyber Intelligence Sharing and Protection Act

(Rep. Rogers, R-MI, and Rep. Ruppersberger, D-MD)

Both government and private companies need cyber threat information to allow them to identify, prevent, and respond to malicious activity that can disrupt networks and could potentially damage critical infrastructure. The Administration believes that carefully updating laws to facilitate cybersecurity information sharing is one of several legislative changes essential to protect individuals' privacy and improve the Nation's cybersecurity. While there is bipartisan consensus on the need for such legislation, it should adhere to the following priorities: (1) carefully safeguard privacy and civil liberties; (2) preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and (3) provide for appropriate sharing with targeted liability protections.

The Administration recognizes and appreciates that the House Permanent Select Committee on Intelligence (HPSCI) adopted several amendments to H.R. 624 in an effort to incorporate the Administration's important substantive concerns. However, the Administration still seeks additional improvements and if the bill, as currently crafted, were presented to the President, his senior advisors would recommend that he veto the bill. The Administration seeks to build upon the continuing dialogue with the HPSCI and stands ready to work with members of Congress to incorporate our core priorities to produce cybersecurity information sharing legislation that addresses these critical issues.

H.R. 624 appropriately requires the Federal Government to protect privacy when handling cybersecurity information. Importantly, the Committee removed the broad national security exemption, which significantly weakened the restrictions on how this information could be used by the government. The Administration, however, remains concerned that the bill does not require private entities to take reasonable steps to remove irrelevant personal information when sending cybersecurity data to the government or other private sector entities. Citizens have a right to know that corporations will be held accountable – and not granted immunity – for failing to safeguard personal information adequately. The Administration is committed to working with all stakeholders to find a workable solution to this challenge. Moreover, the Administration is confident that such measures can be crafted in a way that is not overly onerous or cost prohibitive on the businesses sending the information. Further, the legislation should also explicitly ensure that cyber crime victims continue to report such crimes directly to Federal law enforcement agencies, and continue to receive the same protections that they do today.

The Administration supports the longstanding tradition to treat the Internet and cyberspace as civilian spheres, while recognizing that the Nation's cybersecurity requires shared responsibility from individual users, private sector network owners and operators, and the appropriate collaboration of civilian, law enforcement, and national security entities in government. H.R. 624 appropriately seeks to make clear that existing public-private relationships – whether

voluntary, contractual, or regulatory – should be preserved and uninterrupted by this newly authorized information sharing. However, newly authorized information sharing for cybersecurity purposes from the private sector to the government should enter the government through a civilian agency, the Department of Homeland Security.

Recognizing that the government will continue to receive cybersecurity information through a range of civilian, law enforcement, and national security agencies, legislation must promote appropriate sharing within the government. As stated above, this sharing must be consistent with cybersecurity use restrictions, the cybersecurity responsibilities of the agencies involved, as well as privacy and civil liberties protections and transparent oversight. Such intra-governmental sharing and use should not be subject to undue restrictions by the private sector companies that originally share the information. To be successful in addressing the range of cyber threats the Nation faces, it is vital that intra-governmental sharing be accomplished in as near real-time as possible.

The Administration agrees with the need to clarify the application of existing laws to remove legal barriers to the private sector sharing appropriate, well-defined, cybersecurity information. Further, the Administration supports incentivizing industry to share appropriate cybersecurity information by providing the private sector with targeted liability protections. However, the Administration is concerned about the broad scope of liability limitations in H.R. 624. Specifically, even if there is no clear intent to do harm, the law should not immunize a failure to take reasonable measures, such as the sharing of information, to prevent harm when and if the entity knows that such inaction will cause damage or otherwise injure or endanger other entities or individuals.

Information sharing is one piece of a larger set of legislative requirements to provide the private sector, the Federal Government, and law enforcement with the necessary tools to combat the current and emerging cyber threats facing the Nation. 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: (1) strengthens the Nation's critical infrastructure's cybersecurity by promoting the establishment and adoption of standards for critical infrastructure; (2) updates laws guiding Federal agency network security; (3) gives law enforcement the tools to fight crime in the digital age; and (4) creates a National Data Breach Reporting requirement.

* * * * * * *