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. 1560 - Protecting Cyber Networks Act
(Rep. Nunes, R-California, and 8 cosponsors)

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 Permanent Select Committee on Intelligence on its efforts to craft cybersecurity information sharing legislation and appreciates its efforts to address several of the Administration's most significant concerns. This work has strengthened the legislation and incorporated important changes to better protect privacy. Several improvements to the bill are needed to ensure that it appropriately encourages and facilitates information sharing while safeguarding individuals' privacy interests and civil liberties. As a result, the Administration recognizes the importance of the House and Senate working together to achieve these shared goals and supports House passage of H.R. 1560, 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. 1560'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. In addition, while H.R. 1560 would require that entities take reasonable measures to remove unnecessary personal information before sharing such information with others, the breadth of the liability protections could provide immunity to entities that are grossly negligent or even reckless. The bill's language should also ensure that information is not shared for anticompetitive purposes. The Administration believes that a reasonable solution that strikes an appropriate balance can be found.

Newly authorized cybersecurity information sharing should preserve the long-standing, respective roles and missions of civilian and intelligence agencies. H.R. 1560 permits information sharing with the Federal Government through numerous Federal departments. The Administration supports authorizing new liability-protected sharing relationships through the National Cybersecurity and Communication Integration Center, a civilian entity within the Department of Homeland Security. This approach will help protect privacy, provide for

appropriate transparency, and be more effective operationally, enhancing the Federal Government's ability to quickly integrate, analyze, and use the information to protect the Nation's networks.

H.R. 1560 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 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 these concerns.

H.R. 1560 recognizes that cybersecurity requires a whole-of-government approach and that information must be appropriately shared within the Federal Government. 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 commends the Committee for requiring that intra-governmental sharing be governed by a set of policies and procedures developed by the Federal Government to protect privacy and civil liberties. The Administration seeks to work with Congress to ensure that other language in the bill regarding the ability to modify such information does not interfere with the Federal Government's ability to implement privacy protective policies and procedures.

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.

* * * * * * *