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

April 25, 2012
(House Rules)

STATEMENT OF ADMINISTRATION POLICY

H.R. 3523 - Cyber Intelligence Sharing and Protection Act

(Rep. Rogers, R-MI, and 112 cosponsors)

The Administration is committed to increasing public-private sharing of information about cybersecurity threats as an essential part of comprehensive legislation to protect the Nation's vital information systems and critical infrastructure. The sharing of information must be conducted in a manner that preserves Americans' privacy, data confidentiality, and civil liberties and recognizes the civilian nature of cyberspace. Cybersecurity and privacy are not mutually exclusive. Moreover, information sharing, while an essential component of comprehensive legislation, is not alone enough to protect the Nation's core critical infrastructure from cyber threats. Accordingly, the Administration strongly opposes H.R. 3523, the Cyber Intelligence Sharing and Protection Act, in its current form.

H.R. 3523 fails to provide authorities to ensure that the Nation's core critical infrastructure is protected while repealing important provisions of electronic surveillance law without instituting corresponding privacy, confidentiality, and civil liberties safeguards. For example, the bill would allow broad sharing of information with governmental entities without establishing requirements for both industry and the Government to minimize and protect personally identifiable information. Moreover, such sharing should be accomplished in a way that permits appropriate sharing within the Government without undue restrictions imposed by private sector companies that share information.

The bill also lacks sufficient limitations on the sharing of personally identifiable information between private entities and does not contain adequate oversight or accountability measures necessary to ensure that the data is used only for appropriate purposes. Citizens have a right to know that corporations will be held legally accountable for failing to safeguard personal information adequately. The Government, rather than establishing a new antitrust exemption under this bill, should ensure that information is not shared for anti-competitive purposes.

In addition, H.R. 3523 would inappropriately shield companies from any suits where a company's actions are based on cyber threat information identified, obtained, or shared under this bill, regardless of whether that action otherwise violated Federal criminal law or results in damage or loss of life. This broad liability protection not only removes a strong incentive to improving cybersecurity, it also potentially undermines our Nation's economic, national security, and public safety interests.

H.R. 3523 effectively treats domestic cybersecurity as an intelligence activity and thus, significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres. The Administration believes that a civilian agency – the Department of Homeland Security – must have a central role in domestic cybersecurity, including for conducting and

overseeing the exchange of cybersecurity information with the private sector and with sector-specific Federal agencies.

The American people expect their Government to enhance security without undermining their privacy and civil liberties. Without clear legal protections and independent oversight, information sharing legislation will undermine the public's trust in the Government as well as in the Internet by undermining fundamental privacy, confidentiality, civil liberties, and consumer protections. The Administration's draft legislation, submitted last May, provided for information sharing with clear privacy protections and strong oversight by the independent Privacy and Civil Liberties Oversight Board.

The Administration's proposal also provided authority for the Federal Government to ensure that the Nation's critical infrastructure operators are taking the steps necessary to protect the American people. The Congress must also include authorities to ensure our Nation's most vital critical infrastructure assets are properly protected by meeting minimum cybersecurity performance standards. Industry would develop these standards collaboratively with the Department of Homeland Security. Voluntary measures alone are insufficient responses to the growing danger of cyber threats.

Legislation should address core critical infrastructure vulnerabilities without sacrificing the fundamental values of privacy and civil liberties for our citizens, especially at a time our Nation is facing challenges to our economic well-being and national security. The Administration looks forward to continuing to engage with the Congress in a bipartisan, bicameral fashion to enact cybersecurity legislation to address these critical issues. However, for the reasons stated herein, if H.R. 3523 were presented to the President, his senior advisors would recommend that he veto the bill.

* * * * * * *