

THE FINANCIAL SERVICES ROUNDTABLE

Financing America's Economy



1001 PENNSYLVANIA AVE., NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
TEL 202-289-4322
FAX 202-628-2507

E-Mail info@fsround.org
www.fsround.org

October 6, 2011

Congressman Mac Thornberry
2209 Rayburn House Office Building
Washington, D.C. 20515

Congressman Bob Latta
1323 Longworth House Office Building
Washington, D.C. 20515

Congressman Robert Aderholt
2264 Rayburn House Office Building
Washington, D.C. 20515

Congressman Dan Lungren
2313 Rayburn House Office Building
Washington, D.C. 20515

Congressman Jason Chaffetz
1032 Longworth House Office Building
Washington, D.C. 20515

Congressman Michael McCaul
131 Cannon House Office Building
Washington, D.C. 20515

Congressman Mike Coffman
1222 Longworth House Office Building
Washington, D.C. 20515

Congressman Tim Murphy
322 Cannon House Office Building
Washington, D.C. 20515

Congressman Bob Goodlatte
2240 Rayburn House Office Building
Washington, D.C. 20515

Congressman Steve Stivers
1007 Longworth House Office Building
Washington, D.C. 20515

Congressman Robert Hurt
1516 Longworth House Office Building
Washington, D.C. 20515

Congressman Lee Terry
2331 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressmen,

The Financial Services Roundtable appreciates your leadership of the House Republican Cybersecurity Task Force ("Task Force"). We support efforts to protect the U.S. government, companies and consumers from the increasing threats of cybercrime, while maintaining consumer convenience. Specifically, we offer our comments on the Task Force's October 4 report.

Overall, we support the recognition of the critical role of cybersecurity in today's interconnected economy. We urge the relevant Committees of jurisdiction to work together to develop individual pieces of legislation that complement each other and do not develop disparate and conflicting requirements. We believe the House leadership should manage this process to ensure the results are favorable and that individual Committees do not become duplicative or onerous in their proposals.

Development of Cybersecurity Standards

We applaud the Task Force for encouraging the private sector to participate in the development of standards. We believe the public-private partnerships should start by evaluating the existing standards of the sector. For example, the financial services sector follows standards established by their regulators in accordance with the Gramm-Leach-Bliley Act of 1999 ("GLB").

The Task Force recognized the GLB standard, and, as the public-private partnerships consider new standards, it should use GLB as a model. We believe those compliant with GLB should be exempt from any new standards.

The suggested option of granting those compliant with any new developed standards as compliant with the already existing standards will be quite complex and costly for both the regulators and institutions in implementation. We believe that should the Congress determine that new standards are appropriate, then the new and existing standards should be harmonized to avoid conflicts and redundancies.

Targeted and Limited Regulation of Currently Regulated

We support the statement of the Task Force to target regulations to specific critical functions or facilities, rather than entire organizations. This will help to ensure that the appropriate amount of focus and funding can be used to appropriately protect the critical points of institutions. We agree with the Task Force that the private industry should be involved in the identification of these critical points.

We support the idea of liability protection for compliance and encourage further discussion on this issue, so that it can be further defined and address all industry concerns. The inclusion of liability protection will help to incentivize the involvement of the private sector.

We strongly agree with the sector-specific regulators continuing to have oversight of their institutions on this issue. By utilizing the sector-specific regulators, the additional requirements will be able to enter the environment in a seamless, efficient fashion.

Information Sharing and Public-Private Partnerships

We agree with the Task Force that increased information sharing is key to the continued protection of the cyber ecosystem. We encourage any legislation to utilize existing mechanisms for information sharing. For example in the financial services sector, institutions rely on the Financial Services Information Sharing and Analysis Center (FS-ISAC) to share critical information about cyber attacks. The creation of a mechanism for information sharing would be highly unfavorable and would conflict with the already established entities, such as FS-ISAC.

In addition, we believe that information needs to be shared across sectors in a secure fashion. We consider the recommendation of the Task Force to be a viable recommendation. However, this will require a high level of security, as any database of threat information may be highly targeted.

Updating Existing Cybersecurity Laws

In general, we support changes and updates to cybersecurity laws. We specifically believe that there is a need to strengthen the Criminal Statutes to allow for more severe punishments of cyber criminals. We also support the inclusion of computer fraud racketeering in the Racketeer Influenced and Corrupt Organization law.

We caution the inclusion of concealment of breach into the criminal code. The definition must allow for institution decision makers to evaluate the breach, determine the need for notification and assure notifications are informative and accurate.

In conclusion, we support the efforts of the Task Force to develop these recommendations in an effort to secure the nation's cyber ecosystem. We appreciate your consideration of our comments and welcome the opportunity to discuss further.

Best regards,



Steve Bartlett
President and CEO
The Financial Services Roundtable



Paul Smocer
President
BITS