Overview of McCaul, Rogers, Issa and Hall Cybersecurity Legislation Scheduled for Votes April 27, 2012

H.R. 2096 (McCaul)
Cybersecurity Enhancement Act of 2012

- Addresses the comprehensive cybersecurity needs of the Nation, including evolving cyber threats, by strengthening agency coordination and cooperation on cybersecurity research and development efforts.

- Provides strategic planning for federal cybersecurity R&D plans across the federal government.

- Reauthorizes existing research and education programs at the National Science Foundation (NSF) for three years (FY2013-FY2015) while repealing unused and unnecessary programs.

- Enhances NSF cybersecurity scholarship program to increase the size and skills of the cybersecurity workforce and calls for assessment of current and future cybersecurity workforce needs across the federal government.

- Strengthens National Institute of Standards and Technology (NIST) efforts in the areas of cybersecurity technical standards and cybersecurity education and awareness.

- Puts in place a university-industry task force to explore possible options for carrying out public-private cybersecurity research partnerships.

- Updates the Cybersecurity Research and Development Act and the National Institute of Standards and Technology Act as recommended by the House Republican Cybersecurity Task Force.

- CBO estimates H.R. 2096 does not affect direct spending, and contains no unfunded mandates.

H.R. 3523 (Rogers)
Cyber Intelligence Sharing and Protection Act

Changes that have been made to H.R. 3523

- Narrowing the definition of "cyber threat information" by removing references to intellectual property

- Clarifying that the bill does not authorize the federal government to block accounts, access to websites, or web content

- Permitting lawsuits against the federal government for any violations of the bill's restrictions on information sharing

Specifically

- First, an amendment proposed by the Chairman and Ranking Member that added significant civil liberties and privacy protections was adopted at committee markup and includes an anti-tasking provision and an anti-quid pro quo provision to prevent any attempt to make this bill a surveillance program, as well as an anti-data mining provision and use limitation to restrict how the government may search and use any data voluntarily provided by the private sector.

- Second, an amendment offered by Congressman Mike Thompson (D-CA) was adopted at committee and provides for an independent, detailed review of the federal government's use of voluntarily shared information by the Inspector General to be provided to Congress on an annual basis.

- In addition, a number of new changes are being considered for the legislation as it moves to the House floor, including provisions to give a more prominent role to the Department of Homeland Security, permitting lawsuits against the federal government if the government improperly uses information voluntarily provided by the private sector, and provisions to clarify that no new authority is being provided to the Department of Defense or the Intelligence Community to direct or require public or private sector cybersecurity efforts.

Commonly Asked Questions About CISPA

Q: I've heard that the bill has no protections for privacy and civil liberties; is that right?

A:

- No. To the contrary, the bill contains strong, customized privacy protections designed to ensure that the bill remains centrally focused on protecting cybersecurity.

- First, the bill is completely voluntary; no one is required to change anything about what they do today as a result of the legislation.
- Second, the bill focuses on cyber threat information sharing, allowing the government to provide classified cyber threat intelligence to the private sector and permitting the private sector to identify and share cyber threat information on a voluntary basis.
- Third, the bill only permits information directly pertaining to threats or vulnerabilities to be identified and shared only for the purpose of protecting systems and networks from such threats or vulnerabilities.
- Fourth, the bill authorizes (and encourages) the private sector to anonymize or minimize the cyber threat information it voluntarily shares with others, including the government.
- Fifth, if the cyber threat information is voluntarily shared with the government, there are strong limitations on the government's use of the information.
- The cyber threat information must be protected from disclosure outside the federal government unless further sharing is specifically authorized by the entity providing the information.
- The government may not search the cyber threat information for non-cybersecurity or national security information. (Amendment at markup)
- The government may not use the cyber threat information for other purposes unless a significant cybersecurity or national security purpose exists. (Amendment at markup)
- The government may not require any entity to share cyber threat information with the government. (Amendment at markup)
- The government may not require the sharing of cyber threat information in exchange for government cyber threat intelligence. (Amendment at markup)

- Sixth, if the government violates any of the restrictions placed on it by the legislation, it can be held liable for damages, costs, and attorney's fees through federal lawsuits. (New provision).

Q: Some have said that the bill permits the government to engage in a wide-ranging surveillance program; is that true?

A:

- No. The bill does not permit government surveillance. It allows the government to share classified threat information with the private sector to help the private sector better defend its own networks; the bill also provides clear authority to the private sector—not the government—to identify and share cyber threats on its own systems and networks.

- The bill only permits such private sector identification and sharing of cybersecurity threat information where a company is engaged in the protection of its own systems or networks or those of a corporate customer; it does not permit the monitoring of individual customers.

- The bill does not require anyone to provide information to the government; any sharing of information with others—whether in the private sector or in government—is completely voluntary.

- Rather than requiring information to be provided to the government, the bill explicitly bars the government from requiring private companies to provide it information. (Amendment at markup)

- Moreover, the bill also specifically prohibits the government from offering intelligence only if the private sector provides information back; rather, the government must provide useful intelligence to the private sector regardless of whether it receives any information back from the private sector. (Amendment at markup)

- Indeed, if the government violates either of these prohibitions—or various other restrictions in the legislation—the bill makes the government liable for damages, costs, and attorney's fees in a federal court action. (New provision)

- As such, the government's only role under the bill is to provide intelligence information to the private sector to help the private sector to protect itself and to provide assistance if the private sector voluntarily chooses to provide information to the government.

- In addition, the bill specifically permits the private sector to restrict the cyber threat information it shares, including anonymizing or minimizing the data shared with the government.

- And the bill lets the private sector share as much or as little cyber threat information as it wants and allows the private sector to hold back any sensitive information it deems appropriate.

H.R. 3834 (Hall)
Advancing America's Networking and Information Technology Research and Development Act of 2012

- Reauthorizes the Networking and Information Technology Research and Development (NITRD) program, the federal government's central R&D investment portfolio for unclassified networking, computing, software, cybersecurity, and related information technologies. NITRD includes 15 member agencies, and more than a dozen other participating agencies.

- Specific to cybersecurity, the NITRD program focuses on R&D to detect, prevent, resist, respond to, and recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer-and network-based systems.

- Implements recommendations from the President's Council of Advisors on Science and Technology (PCAST) including improving interagency coordination and planning with input from policy and technical experts.

- Rebalances R&D portfolios to focus less on short-term goals and place more emphasis on large-scale, long-term interdisciplinary research.

- Updates research areas to reflect new terminologies.

- Puts in place a university-industry task force to explore possible options for carrying out public-private cyber-physical systems research partnerships.

- Convenes an interagency working group to identify cloud computing research gaps and examine the potential for using the cloud for federally funded research.

- Updates the High Performance Computing Act of 1991 as recommended by the House Republican Cybersecurity Task Force.

- CBO estimates implementing H.R. 3834 does not affect direct spending, and contains no unfunded mandates.

H.R. 4257 (Issa)
The Federal Information Security Amendments Act of 2012

- Enhances the Federal Information Security Management Act (FISMA) of 2002 by

improving the framework for ensuring security over information technology systems that support the federal government.

- It establishes a mechanism for stronger oversight through a focus on automated and continuous monitoring of cybersecurity threats and the implementation of regular threat assessments.

- Currently, federal agencies are struggling with cyber-security threats, and this update to FISMA will incorporate the last decade of technological innovation, while also addressing FISMA shortcomings realized over the past years.

# # #