WebMemo
Published by The Heritage Foundation
No. 2490
June 17, 2009

The SAFETY Act: Obama Cyber Plans and the Private Sector

Jena Baker McNeill

On May 29, the Obama Administration released the results of its 60-day cyber review. The review correctly emphasized the vital role of the private sector in any future national cybersecurity strategy. Involving the private sector effectively, however, will require a liability protection regime—one that encourages industry to invest in cybertechnologies that protect against acts of cyberterrorism.

This can best be accomplished by the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, which provides liability protection for manufacturers whose products and services are used in combating terrorism. Congress should support the continuance and expansion of the SAFETY Act, and the Administration should ensure that the act's protections are used effectively in the cyber realm.

The Cybersecurity Review. President Obama ordered a 60-day review of the nation's cybersecurity efforts in February. Major cyberattacks, including one on the nation of Georgia, and a constant barrage of hackings on major financial institutions and retailers like T. J. Maxx and Marshalls (a hacker stole $45.7 million in credit and debit cards in 2007) have led the drive for a comprehensive assessment of cyber capabilities, challenges, and recommendations going forward.

The review highlights several major aspects of the national cyber realm, including the role of the federal government, a description of the nation's cyber problem, and recommendations for the future. The role of the private sector in helping to tackle the problem was also well documented in the review, including the need for more federal government–private sector partnerships.

The review further noted the need to continually invest and research new technologies to stop cyberattacks. Specifically, it called for the federal government to "harness the full benefits of technology to address national economic needs and national security requirements." But the review emphasized the private sector's role in meeting this goal.

The Importance of the Private Sector in Cyber Protection. The private sector remains a pivotal partner in ensuring the safety of cyber infrastructure for the following reasons:

- Almost all cyber infrastructure is owned and maintained by the private sector;
- Cybertechnologies are used in almost every element of human life—from ATMs to medical technologies; and
- The private sector can research and develop new technologies at a faster rate than the federal government.

Even with the financial benefits of developing new cybertechnologies, the private sector will not

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandSecurity/wm2490.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

invest in these new technologies if the benefits of doing so are outweighed by the risks. For example, companies are less likely to create and market a new product if a lawsuit stemming from it could destroy their entire business.

After the 1993 World Trade Center bombing, the New York Supreme Court upheld a decision that found the Port Authority of New York and New Jersey liable for the bombing. The court's reasoning: The Port Authority was aware of the threat and did not take reasonable steps to mitigate it. After 9/11, insurance premiums for terrorism-related risks skyrocketed, and a number of firms stopped offering terrorism insurance. This kind of liability and potentially devastating jury verdicts have made many companies hesitant to research, develop, and market anti-terrorism technologies.

But America simply cannot afford to let the private sector stop innovating. Recognizing this problem, Congress enacted the SAFETY Act, which lowered the liability risks of manufacturers that provide products and services used in combating terrorism by giving government-certified technologies protection from suit if the technology failed or was involved in an act of terrorism. The SAFETY Act applies to a multitude of anti-terrorism technologies and includes those used to ward off cyberattacks.

How to Involve the Private Sector. The SAFETY Act continues to play an important role in ensuring that the U.S. does not lose its footing in the cyber domain. America needs companies to continue to develop technologies that keep the U.S. safer, both physically and virtually. As part of a future cyberstrategy, the Obama Administration should:

- *Support the SAFETY Act.* Over 200 companies have obtained SAFETY Act certification. The Department of Homeland Security (DHS) must continue to encourage new applicants for SAFETY Act certification. This approach needs to include aggressive marketing, especially to small businesses and specifically to cyber businesses. Neither DHS nor the private sector can assume that Congress will allow the SAFETY Act to stand over time, and it must be continually maintained.
- *Go international.* One area that is ripe for enhanced international cooperation is third-party liability for terrorist attacks. The SAFETY Act provides protections for "sellers" (manufacturers, distributors, and providers) for cases under the jurisdiction of U.S. courts. Terrorism, however, is a global threat, and homeland security is a global mission. From securing the border to protecting global supply chains, virtually every aspect of preventing terrorist attacks has an international dimension that requires the U.S. to work effectively with its friends and allies. Other countries should consider similar liability protection regimes to provide the industrial base around the world with incentives to develop and adopt the best tools to fight terrorism no matter where they are manufactured or employed. The U.S. should support these kinds of partnerships on a bilateral basis.
- *Streamline the assessment process.* DHS has gone to great lengths to make sure that the SAFETY Act process continues to be company-friendly. But the departments needs to ensure that the auditing program is not too burdensome and that it is reflective of business needs while verifying that only quality products obtain certification.

Support the Private Sector. The Obama Administration is right to place attention on America's cyber challenges. But it is vital to recognize the principal position of the private sector in ensuring cybersecurity. The Administration should be careful not to view the private sector as simply another partnership: It is a major player in the cyber domain whose efforts must be supported.

—Jena Baker McNeill is Policy Analyst for Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.