The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3741 | SEPTEMBER 24, 2012

Cybersecurity: The Latest Research and Analysis

The Heritage Foundation

In the age of modern warfare, the threat of a cyber attack is often overlooked. Focus tends to lie more on physical threats, such as missile defense and nuclear weapons. However, one of the greatest threats to national security is a lack of cybersecurity. Politicians have tried to bring legislation to the floor in an effort to "do something" to protect the nation from these threats, but most of these bills would cause far more harm and provide little protection.

The Heritage Foundation has recently published a number of *Issue Briefs* and blog posts analyzing the Obama Administration's policies and congressional proposals on cybersecurity. These writings cover the President's recent draft executive order, legislation, and whether the government is better able than the private sector to protect against cyber attacks.

This paper, in its entirety, can be found at **http://report.heritage.org/ib3741**

Produced by The Heritage Foundation

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

President Obama's Executive Order

Executive Orders in Cybersecurity Result in Incomplete and Empty Solutions
David Inserra
September 10, 2012

http://blog.heritage.org/2012/09/10/executive-orders-in-cybersecurity-result-in-incomplete-and-empty-solutions/

In early September, a draft of a cybersecurity executive order was shown to members of the press. Leaked reports of secretive decision-making are what the U.S. gets when the President decides to ignore the democratic process and implement rules by executive fiat. The U.S. also gets policies that are often incomplete and poorly thought out.

The executive order has its limits, and one of them is that it cannot provide liability protection. Effective information sharing can be realized with actual legislation, but it would help if the President would slow down and allow Congress to do its job of crafting a complete approach.

Legislation

A Cybersecurity Offer Companies Can't Refuse
Paul Rosenzweig
September 24, 2012

http://blog.heritage.org/2012/09/24/a-cybersecurity-offer-companies-cant-refuse/

In a remarkable letter to all *Fortune* 500 CEOs, Senator Jay Rockefeller (D–WV) bemoans the business community's opposition to his cybersecurity legislation, the Cybersecurity Act of 2012. He is shocked—simply shocked, as was Captain Renault in *Casablanca*—that any business institution could possibly oppose more government red tape when "security" is on the line.

An even more notable aspect of the Senator's letter is the deeply detailed set of questions about the *Fortune* 500 companies' cybersecurity polices. He asks each company whether it has cybersecurity practices, when they were developed, how they were developed, how frequently they are updated, and whether the federal government played any role in developing them. The Senator also asks three questions that can best be paraphrased as "please tell me what could possibly be wrong with my highly reasonable legislation and why you disagree with me when I am so obviously right."

Cybersecurity Act of 2012: Revised Cyber Bill Still Has Problems
Paul Rosenzweig

July 23, 2012

http://www.heritage.org/research/reports/2012/07/cybersecurity-act-of-2012-revised-cyber-bill-still-has-problems

In July, Senators Joseph Lieberman (I–CT) and Susan Collins (R–ME) released a revised version of their Cybersecurity Act of 2012. The bill was voted down prior to Congress leaving for their annual August recess. Though an able effort, the revised bill still had grave problems that would likely chill innovation without improving cybersecurity.

Congress thankfully rejected the effort to create a new regulatory system for cybersecurity. Instead, cybersecurity legislation should strengthen protections for private-sector actors in order to authorize and incentivize the sharing of cyber threat and vulnerability information. The latest offering from Senators Lieberman and Collins did neither of these things.

Updated: Comparison of Cybersecurity Legislation
The Heritage Foundation
July 24, 2012

http://www.heritage.org/research/factsheets/2012/07/updated-comparison-of-cybersecurity-legislation

During the summer of this year, Congress considered several cybersecurity bills. The Cyber Intelligence Sharing and Protection Act (CISPA) passed the House in April, and two Senate bills—the Cybersecurity Act of 2012, authored by Senators Joseph Lieberman (I–CT) and Susan Collins (R–ME), and the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (SECURE IT), authored by Senator John McCain (R–AZ)—were defeated.

Estimates of losses from cyber theft vary widely and may be as high as $400 billion in the West annually. The specter of a crippling attack on critical industries, such as the electrical grid or the financial system, looms in the minds of many. Congress should not act before it considers the consequences of each bill. Within the bills are competing views on how to solve the nation's cybersecurity problems, and each deserves closer inspection.

Government Involvement

The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government
Paul Rosenzweig
May 24, 2012

http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government

As the Senate continues its debate over cybersecurity legislation, one of the most important questions it will have to address is whether the federal government, acting through the Department of Homeland Security (DHS), should play a significant role in crafting cybersecurity regulations that will govern activities of the private sector as well as of government. Proponents of such a role, embodied in Title I of the Lieberman–Collins Cybersecurity Act of 2012, contend that the private sector has done an inadequate job of protecting itself and that market incentives have not developed appropriately to promote self-protection. Opponents of Title I argue that the government is ill equipped to develop effective cybersecurity regulations and that the regulatory process is too cumbersome for the development of rules and standards applicable to the dynamic cyber domain.

The federal government's record on cybersecurity does not inspire confidence that it can provide a solution to the cybersecurity threats faced by the private sector. Cybersecurity should be a cooperative effort between the private sector and the government, with each contributing in its own way. The government is in a position to collect and share important cybersecurity threat and vulnerability information, while the private sector can innovate and share information as well.

The State of Privacy and Security: Our Antique Privacy Rules
Paul Rosenzweig
August 1, 2012

http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules

Rather than vainly trying to stop progress or trying to fit new technologies into old principles of privacy that no longer apply, Congress needs to answer the hard policy questions regarding cybersecurity. Instead of reflexively opposing technological change, a wiser strategy is to accept the change and work within it to channel change in beneficial ways.

This will require a rethinking of privacy—both a reconception of what we think it means and a reconfiguration of how we think it is to be protected. It may be true that "privacy is dead," but for those who truly want to protect privacy, the motto should be: "Privacy is dead. Long live the new privacy."