WebMemo
Published by The Heritage Foundation
No. 3488
February 6, 2012

Promoting Cybersecurity Through the PRECISE Act

Paul Rosenzweig

Earlier this year, The Heritage Foundation noted the positive features of the Rogers Ruppersberger bill (H.R. 3523), a solid cybersecurity bill that was the product of the House Select Committee on Intelligence and passed out of that committee on a 17 1 vote.[1]

Another bill, the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act, or PRECISE (H.R. 3674), is sponsored by Representative Dan Lundgren (R–CA) and has bipartisan support in the House Homeland Security Committee, where it will soon be considered by the full committee. The similarities and differences between the two bills illuminate issues of concern in the cybersecurity debate.

DHS as Lead Agency. The PRECISE bill gives the Secretary of Homeland Security a leading role in cybersecurity. The Department of Homeland Security (DHS) is given responsibility for maintaining a clearinghouse of cyber threat information and disseminating that information broadly within the federal government and to the private sector. Thus, under the Lundgren bill, the civilian sector would lead in cybersecurity, rather than the military.

More than a year ago, in setting out 10 conservative principles to guide cybersecurity legislation, Heritage asserted that this is probably the correct choice.[2] While the National Security Agency (NSA) currently has greater capacity for cybersecurity efforts than DHS, in the long run, the strong preference should be a civilian response for what is, after all, a predominantly civilian network. The civilian effort will rely at its core on existing expertise that is predominantly with NSA, but the fundamental preference for civilian control is a wise one. Any other choice would be fraught with political tension and practical difficulties.

Private-Sector Information Sharing. Interestingly and creatively PRECISE also creates a nonprofit private-sector corporation to manage the private-to-private aspects of cyber threat information sharing. The new National Information Sharing Organization (NISO) would be managed by a joint public-private board of directors with additional representation from privacy and civil-liberties nongovernmental organizations. It would be charged with enabling private-sector cyber threat information sharing, but only with significant privacy protections.

This course, too, follows some of Heritage's earlier recommendations. We have urged the formalization of a public-private partnership for cyber defense by creating a congressionally chartered nonprofit corporation (akin to the American Red Cross and the

This paper, in its entirety, can be found at:
http://report.heritage.org/wm3488

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

Millennium Challenge Corporation).[3] The NISO proposed in H.R. 3674 is very much a close relative of this proposal and an idea worthy of consideration.

This potential organization would address many of the concerns that have frustrated the purely private or public responses. It would eliminate the first mover economic problem by federalizing the response, and it would allow greater maintenance of the security of classified information within the sphere of a government corporation. As a corollary, the quasi-public nature of the NISO will provide a forum in which defense-related private-sector information could be shared without fear of compromise or competitive disadvantage. Thus, the NISO would provide a secure platform allowing the government and the private sector to fully utilize their information assurance capabilities.

Which Data and With Whom? There is, however, one area of cybersecurity where the PRECISE Act makes a modest misstep in taking an overly narrow view. The Lungren bill identifies a specific, limited category of cyber threat information that can be shared. It authorizes the new NISO to share only information necessary to describe a method of defeating technical controls on a system or network that corresponds to a cyber theat.

This is an unnecessarily limited definition. The Rogers bill, by contrast, has a broader definition of a cyber threat and authorizes sharing any information pertaining to the protection of a system against efforts to degrade, disrupt, or destroy the system or to prevent theft or misappropriation of information from the system.

Doubtless, the Lungren bill drew its narrow definition in an effort to secure the support of the privacy and civil liberties communities. But in doing so, it runs the risk of resurrecting old and discredited ideas of limiting the ways in which intelligence information can be shared within the federal government. By narrowing the definition of what can be shared, the PRECISE Act would, in effect, recreate the stovepipe mentality and segregate cyber threat information from other types of intelligence collection and analysis. The Rogers Ruppersberger bill, on the other hand, would permit cyber threat information to be aggregated with other intelligence data as a means of further connecting the dots.

The better way to achieve the same objective is to enable a strong oversight function. Instead of limiting which information can be shared and with whom, the wiser course is to allow a broader ability to connect the dots but use a careful and vigorous oversight program to make sure that those who are entrusted with the data do not misuse it.

A Non-Regulatory Approach. Both the PRECISE Act and the Rogers Ruppersberger bill are far less directive and mandatory than their Senate counterparts, which will soon come to the floor of that chamber. The Rogers bill has no regulatory structure at all, while PRECISE has a comparatively light, risk-assessment and standards-based approach that would be significantly less intrusive on the private sector than either the earlier Senate drafts or the Obama Administration proposal. Either House bill, with an emphasis on enabling private-sector action, would serve as a wise guide to forthcoming Senate deliberations.

Paul Rosenzweig is a Visiting Fellow in the Center for Legal and Judicial Studies and 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.

1. Paul Rosenzweig, "Congressional Cyber Initiative Shows Promise," Heritage Foundation *WebMemo* No. 3478, January 31, 2012, at *http://www.heritage.org/Research/Reports/2012/01/Rogers-Ruppersberger-Bill-A-Solid-Cybersecurity-Approach.*
2. Paul Rosenzweig, "10 Conservative Principles for Cybersecurity Policy," Heritage Foundation *Backgrounder* No. 2513, January 31, 2011, at *http://www.heritage.org/research/reports/2011/01/10-conservative-principles-for-cybersecurity-policy.*
3. For a more detailed summary of this idea, see Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence," National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: The National Academies Press, 2010), at *http://books.nap.edu/openbook.php?record_id=12997&page=245.*