The Heritage Foundation
LEADERSHIP FOR AMERICA

# ISSUE BRIEF

No. 3667 | JULY 16, 2012

# Securing U.S. Computer Networks with SECURE IT

*Steven P. Bucci, PhD*

The Heritage Foundation has previously written on the Cybersecurity Act of 2012, authored by Senators Joseph Lieberman (I–CT) and Susan Collins (R–ME),[1] but additional analysis of Senator John McCain's (R–AZ) Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (SECURE IT) is needed.

SECURE IT relies on stronger cybersecurity information sharing than the Lieberman–Collins bill and also rejects potentially costly regulations. Information sharing costs almost nothing and is something that both parties can agree on. Furthermore, information sharing is a continuous and regular process that helps private companies and the federal government keep up with constantly changing cyber threats.

This paper, in its entirety, can be found at **http://report.heritage.org/ib3667**

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

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



## Strong Information-Sharing Provisions Improve Security.

*Definition of Cyber Threat Information.* SECURE IT defines cyber threat information as information that signifies or describes:

- Technical or operation vulnerabilities;
- A measure or effort to mitigate cyber threats;
- Malicious reconnaissance;
- Methods of defeating technical or operational controls;
- Computer activity or protocols "known to be associated with a malicious cyber actor" or threat;
- A method of allowing legitimate users to inadvertently defeat technical or operation controls;
- "The actual or potential harm caused by a cyber incident ... when it is necessary in order to identify or describe a cybersecurity threat";
- Any other attribute of a cyber threat or cyber defense information that would improve awareness if disclosure of such information is not forbidden by law; and
- Any combination of the above features.

This definition is broad and is directed at obtaining as much information related to cyber threats as possible. Such an approach ensures that U.S. cybersecurity analysts and providers have all the relevant information needed to do their jobs effectively.

*Private-to-Private Sharing Mechanisms.* SECURE IT removes any legal ambiguities that currently stand in the way of voluntary information sharing by stating that "notwithstanding any other provision of law," an entity may share cyber threat information with the government or any other entity. Such information-sharing provisions allow the private sector to effectively share cyber threat information with other private entities with no fear of breaking a law.

SECURE IT also allows private-to-private sharers to place restrictions on the use and further sharing of their information to make sure it goes only as far as the sharer wants. Additionally, giving information to

one entity does not give other entities a right to that information. Such provisions ensure that each sharer has the right to determine what and with whom it shares.

*Government-to-Private Sharing and Classification Provisions.* Cyber threat information that the government possesses would be shared with cybersecurity sharing centers located in various government agencies that have cybersecurity responsibilities. These centers would then share classified information with certified entities while sharing declassified and publically available information with all entities that want such information. Establishing multiple cybersecurity centers that are constantly and rapidly sharing with each other can help avoid "stovepiping"—the absence of sharing between different parts of government.

*Liability Protection.* SECURE IT provides sharers with strong liability protection by stating that "no cause of action shall lie or be maintained in any court against any private entity for" the sharing and authorized use of cyber threat information. This statement protects sharers and users of cyber threat information from lawsuits as a result of inadvertently harmful actions (or inactions) taken because of shared information. Additionally, there is no liability for not participating in the program, ensuring that sharing is voluntary.

Liability protection that is weaker than what SECURE IT provides, such as "good faith" protection, would allow additional lawsuits and vastly decrease the amount of shared information. Strong liability protection, such as that provided in SECURE IT, would ensure that the private sector is not afraid to share and use cyber threat information.

*Freedom of Information Act (FOIA), Regulatory Use, and Proprietary Information Protections.* Private-sector actors will not share information if it might be used to regulate them. Additionally, if private actors fear that information they share will be accessible via FOIA, they will share less information, especially if it touches on something sensitive or proprietary. Since cyber threat information sharing is about defending networks and data, SECURE IT also prevents other actors from using shared information to gain an unfair competitive advantage over the sharer.

## Government Roles and Restrictions.

*Use of Shared Information.* SECURE IT clearly delineates how and why the federal government can use cyber threat information. Cyber threat information may be used for any cybersecurity or national security purpose, as well as for the prevention, investigation, or prosecution of any of the offenses in section 2516 of title 18 of the U.S. Code. By allowing such government use, information does not get stovepiped into only certain agencies but is available to all that have a legitimate use for such information.

*Role of the Department of Homeland Security (DHS).* SECURE IT charges DHS with housing one of several cybersecurity centers throughout the federal government. Additionally, DHS will assist with public cyber education efforts and the strengthening of federal information security. As DHS is charged with the defense of critical infrastructure such as power grids, it is wise to have it involved in cybersecurity, though in an ideal world it would take more of a leading role.

*Role of the National Security Agency (NSA) and the Department of Defense (DOD).* The NSA and the DOD would both have a cybersecurity center under SECURE IT. The NSA and the DOD currently have the strongest cyber capabilities, and SECURE IT chooses to lean on these organizations for support. With their superior analytical and technical capabilities, the NSA and the DOD would be able to share helpful cyber threat information with other public and private organizations.

*Privacy Oversight.* SECURE IT states that reasonable privacy protections "through anonymization or other appropriate measures" should be undertaken "while fully accomplishing the objectives" of information sharing. To this end, SECURE IT charges the Privacy and Civil Liberties Oversight Board with issuing a biennial report on the type of information that has been shared, the impact of sharing on privacy, steps taken to reduce sharing's effect on privacy, and any breaches or violations of SECURE IT's use and sharing provisions.

Additionally, the bill provides for Inspector General oversight of cybersecurity centers and federal agencies receiving cyber threat information to review compliance with privacy provisions.

This approach ensures that information sharing would be carried out, but, short of weakening sharing, all reasonable steps will be taken to protect privacy. Instead of inhibiting

1. Paul Rosenzweig, "Senate Cybersecurity Bill: Not Ready for Prime Time," Heritage Foundation *Backgrounder* No. 2661, March 7, 2012, http://www.heritage.org/research/reports/2012/03/senate-cybersecurity-bill-not-ready-for-prime-time.

sharing, SECURE IT uses robust oversight to make sure that information is used appropriately and privacy is reasonably safeguarded.

## Regulations and Costs.

Other than requiring a security clearance for classified information, SECURE IT imposes zero regulations on the private sector. Since the cyber realm is such a dynamic environment, slow, static regulations would likely be unable to keep up. Thus, SECURE IT's approach avoids the pitfall that merely encourages compliance with outdated regulations but does not create real security.

Since there are no mandates or regulations, the cost to the private sector is next to nothing. Some private-sector actors might hold more privacy protections than others, perhaps in response to customer demand, and this might entail small additional costs to those actors. Importantly, such costs are completely optional and will be avoided by most firms. Any minimal costs that are borne by the private sector pass a cost-effectiveness test.

## Strong Protections for Minimal Costs.

SECURE IT improves cyber threat information sharing while rejecting regulations and mandates, which are likely high cost and would result in mere compliance with outdated and obsolete rules. By protecting information sharers from liability, loss of proprietary information, and regulations, SECURE IT ensures that the private sector is actively involved in sharing information.

Cybersecurity centers will ensure that information is shared rapidly with the private sector and federal agencies, and broad government use provisions would allow information to help with legitimate government functions, including national security and law enforcement. Privacy is protected by vigorous oversight bodies, not information-sharing restrictions that would harm the usefulness of sharing.

*—**Steven P. Bucci, PhD,** is Senior Research Fellow for Defense and 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.*