Cybersecurity bill will expand surveillance powers of US military and intelligence agencies

Thomas Gaist
15 July 2014

The Senate Intelligence Committee voted 12-3 last week in favor of the Cybersecurity Information Sharing Act (CISA) of 2014, new legislation that massively expands the data-gathering powers of the US security, intelligence and military bureaucracies, by allowing "voluntary" information sharing between private companies and the government.

The Intelligence Committee "marked up" the bill in two secret sessions closed to the public. The bill, which was drafted by Senators Saxby Chambliss (Republican, Georgia) and Dianne Feinstein (Democrat, California), is now set to go before the chamber as a whole.

CISA clears the way for virtually unrestrained information sharing between the US government and corporations. Under the bill, large quantities of data can be transferred from companies to the Department of Homeland Security (DHS) without any form of legal review, so long as the data is considered "cybersecurity information."

Once acquired from the telecommunications corporations, DHS will then automatically share the data in real time with the US National Security Agency (NSA), Cyber Command (USCYBERCOM), and other sections of the Defense Department (DoD) bureaucracy. The government agencies are authorized to retain data shared in this way indefinitely.

These legislative changes amount to a far-reaching extension of the powers of the military apparatus to intervene in civilian electronic systems. As the New America Foundation (NAF) wrote in its report, "Analysis of the Cybersecurity Information Sharing Act of 2014: A Major Step Back on Privacy, DHS would serve merely as a portal for DOD entities to receive cyber threat indicators, and there would be no functional distinction between sharing with a civilian agency and sharing directly with the NSA." The broad language of CISA, New America wrote, "may be interpreted to authorize the government to gain direct access to a company's information systems to receive cyber threat indicators."

Broad language in CISA leaves the door open for companies to engage in "hack-back" activities, such as deploying malware and spyware on the machines of customers, according to the NAF report. Individuals who are harmed by CISA-based activities have no avenue to address their grievances, since the bill contains strong protections for companies from any liabilities associated with information sharing, protecting them against lawsuits by users whose privacy and democratic rights are violated by such operations.

Exemptions from the Freedom of Information Act (FOIA) and other "sunshine laws" are built into the legislation, shielding the information sharing programs from public scrutiny.

At the same time, the bill hands the US government another powerful weapon for its war against "insider threats" (government terminology for leakers and whistleblowers), allowing for data collected through the mass information sharing to be used for prosecutions launched under the Espionage Act.

The CISA legislation effectively transfers new surveillance powers to domestic police agencies. State and local law enforcement are empowered by CISA to "use, retain, and further share" data obtained through the information sharing program to launch or aid investigations completely unrelated to cybersecurity.

Numerous civil rights and watchdog organizations

© World Socialist Web Site

have announced opposition to the CISA bill. The Center for Democracy in Technology (CDT) described CISA as a "backdoor wiretap," writing that CISA "addresses none of the Snowden revelations about the NSA" and would "funnel more private communications and communications information to the NSA."

Writing for the American Civil Liberties Union (ACLU), Sandra Fulton argued that the CISA bill "poses serious threats to our privacy, gives the government extraordinary powers to silence potential whistleblowers, and exempts these dangerous new powers from transparency laws."

As noted by Fulton, "the definition they are using for the so-called 'cybersecurity information' is so broad it could sweep up huge amounts of innocent Americans' personal data … CISA would circumvent the warrant requirement [established in the Fourth Amendment] by allowing the government to approach companies directly to collect personal information, including telephonic or Internet communications, based on the new broadly drawn definition of 'cybersecurity information.'"

CIPSAisBack.org, a web site dedicated to monitoring US cybersecurity legislation, wrote that the bill "would allow for and encourage sweeping data mining taps on Internet users for the undefined purpose of domestic 'cybersecurity.'"

CISA may also bolster US government efforts to "stockpile vulnerabilities," a practice whereby weaknesses discovered in existing computer networks are not disclosed to the network operators, but instead are recorded for possible future exploitation by teams of government hackers. As revealed by Edward Snowden last summer, Washington has already ordered the hacking of hundreds of civilian targets in China.

Under the auspices of "cybersecurity," the US government is building powerful new components of the national security state, empowered to carry out new forms of surveillance and data acquisition as well as cyber-attacks against computer systems deemed threatening by the government. These powers can be used to shut down web sites, networks, and entire sections of the Internet.

While the Constitution prohibits military and espionage operations inside the US, intelligence officials have openly expressed ambitions to overcome these restrictions.

As a senior intelligence agent told the *New York Times* in 2009 in the lead-up to the launch of the Pentagon's Cyber Command (CYBERCOM), "These attacks start in other countries, but they know no borders. So how do you fight them if you can't act both inside and outside the United States?"

CYBERCOM went operational in May of 2010, under the command of General Keith Alexander. Alexander told the Brookings Institute in 2010 that while CYBERCOMMAND currently plays no role in the nation's civilian networks, in exceptional circumstances an executive order could be issued allowing the DoD-based agency to assume control over civilian information systems.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site