

The Sunshine in Government Initiative

1101 Wilson Boulevard, Suite 1100
Arlington, Virginia 22209
Phone (571) 481-9322

sunshineingovernment.org
info@sunshineingovernment.org
@sunshineingov



June 25, 2014

Senator Dianne Feinstein
Chairman
Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

Senator Saxby Chambliss
Vice Chairman
Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Feinstein, Vice Chairman Chambliss and Members of the Senate Select Committee on Intelligence:

The nine press groups that comprise the Sunshine in Government Initiative (SGI) write to express our grave concerns with the [Cybersecurity Information Sharing Act of 2014 \(CISA\)](#) prior to an expected Committee markup this week. SGI consists of the American Society of News Editors, The Associated Press, Association of Alternative Newsmedia, National Newspaper Association, Newspaper Association of America, Online News Association, Radio-Television Digital News Association, Reporters Committee for Freedom of the Press and Society of Professional Journalists.

We appreciate that the Act's main goal is to encourage private companies, through significant limitations on liability, to share information voluntarily with the federal government (and each other) to help combat cyber threats.

However, we are concerned that the discussion draft released last week would threaten the flow of accurate news and information to the public and policymakers by creating a substantial chilling effect among journalists and their confidential sources, which are sometimes necessary to inform the public about matters that have nothing to do with securing computer networks.¹ CISA as proposed would grant the federal government virtually unlimited authority to thwart newsgathering and the use of confidential sources by removing meaningful judicial oversight and placing the balancing of vital democratic interests in the hands of the executive branch and private industry.

The bill implicates the First and Fourth Amendments, and would permit the government to entirely bypass existing legal standards and prior notice requirements, including those currently found in the Electronic Communications Privacy Act (ECPA). The legislation is also diametrically opposed to the carefully crafted language of the federal shield bill, which tasks federal judges with balancing the right to a free press and the needs of law enforcement.

¹ We have also consistently expressed concerns about overbroad exemptions to disclosure under the Freedom of Information Act in cybersecurity legislation. We encourage this Committee to craft any exemptions as narrowly as possible to reasonably protect corporate proprietary information and personal information, while still enabling the public and press to use FOIA to conduct oversight of the government's cybersecurity efforts.

Specifically, CISA would authorize any department or agency of the federal government to obtain from private companies – *without a warrant or other traditional legal process* – “cyber threat indicators”² and use that information for a “cybersecurity purpose”³ or for “the purpose of preventing, investigating, or prosecuting” crimes under the Espionage Act (Title 18, Chapter 37).⁴ Notwithstanding the express mention of the Espionage Act, the terms “cyber threat indicator” and “cybersecurity purpose” (and the additional terms that further define these terms) are *exceedingly overbroad*.

Reading the interconnected definitions together, CISA would grant the federal government the authority to engage in the *warrantless collection* of journalists’ communications records – including content *and* transactional metadata – if the government deems the journalists, or the confidential sources they work with, “security vulnerabilities” or “cybersecurity threats” potentially “adversely impacting” the confidentiality of information stored on government computers.

This kind of unbridled federal government authority – to classify journalists and their confidential sources as “security vulnerabilities” or “cybersecurity threats,” and obtain their communications records without meaningful judicial oversight, legal standards or prior notice – would create a significant chilling effect that would harm newsgathering and the ability of the press to inform the public.

The bill’s practical impact would be felt hardest by national security reporters who often inform the public with stories based on unauthorized disclosures of government information. We understand that unauthorized disclosures are disfavored by the government, but they also serve valuable purposes including exposing government malfeasance or outright illegal conduct. *In fact, like other committees in both the Senate and House, this Committee’s oversight activities regularly depend upon and benefit from news reporting based on unauthorized disclosures.*

Yet a national security reporter may fall squarely within the extremely broad definitions of CISA, be deemed a “procedural” or “operational” threat to the continued secrecy of government information, and be subject to government surveillance – either in the form of real-time monitoring or access to stored records – without the specific protections of the Fourth Amendment, ECPA, or even the Foreign Intelligence Surveillance Act (FISA). Or, if a story has already been published based on a leak, the federal government could obtain from private companies communications records about the journalist for the express purpose of investigating or prosecuting the leaker under the Espionage Act.

² “*Cyber threat indicator*” includes “information that indicates, describes, or is necessary to identify . . . a method of defeating a security control or exploitation of a security vulnerability” or “a security vulnerability.” Section 2(8).

“*Security vulnerability*” is “any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.” Section 2(20).

“*Security control*” is “the management, operational, and technical controls used to protect the confidentiality, integrity, and availability of an information system or its information.” Section 2(19).

³ “*Cybersecurity purpose*” – for which the federal government may use “cyber threat indicator” information – is “the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.” Section 2(6).

“*Cybersecurity threat*” is “an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.” Section 2(7).

⁴ Section 5(d)(5)(A).

Current law gives the Justice Department ample authority to obtain communications records to investigate and prosecute Espionage Act violations.

And while the bill gives a nod to whistleblowers,⁵ national security whistleblower protections are weak, especially for contractors, and therefore workers may feel that going to the press with information of vital public interest is their only option.

Simply put, CISA would make it more difficult for journalists to do their jobs while making it easier for the federal government to compromise journalists' confidential sources, including government whistleblowers who may share evidence of government waste, fraud or abuse.

Not only would this kind of government authority frustrate the Constitution and existing laws like ECPA, it would also upend the carefully crafted language in the Free Flow of Information Act (S. 987) that was approved by the Judiciary Committee last September with the support of members of this Committee. The federal shield bill is balanced legislation that would place all requests for confidential source information, whether issued to journalists themselves or their service providers, before federal judges, enabling journalists to protect their sources while enabling law enforcement in appropriate circumstances to get the information they need to prosecute crimes and keep our nation secure.⁶

Additionally, CISA's protections for personal information unrelated to a potential cybersecurity threat, while well-intentioned, would be ineffective. CISA would require a private entity, prior to sharing cyber threat information with the federal government, "to remove any information . . . that is known to be personal information of or identifying a United States person, not directly related to a cybersecurity threat."⁷ Therefore, personal information about a journalist *may* be shared with the federal government if that information is "directly related to a cybersecurity threat," which may include an unauthorized disclosure of government information given that, as discussed above, "cybersecurity threat" includes "an unauthorized effort to adversely impact the . . . confidentiality . . . of an information system or information that is stored on, processed by, or transiting an information system."

Further, while CISA would permit private companies to "voluntarily" share cyber threat information with the federal government, nothing in the bill prohibits the government from proactively *asking* a private company to do so. A company would be free to decline, but a federal agent showing up to a company's office often comes with an air of coercion, increasing the likelihood that a company will comply with the request to avoid the risk of any hassle with the government.

⁵ "Nothing in this Act shall be construed to preempt any employee from exercising rights currently provided under any whistleblower law, rule, or regulation." Section 8(b).

⁶ State shield laws, which seek to protect confidential sources and unpublished newsgathering work product in state cases, and state privacy laws would also give way given that CISA would permit state and local law enforcement agencies to use "cyber threat indicator" information "for the purpose of preventing, investigating, or prosecuting a criminal act" (Section 4(d)(4)) *and* the bill would preempt "any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this Act." Section 8(j).

⁷ Section 4(d)(2).

Finally, CISA would require the attorney general to write guidelines “relating to privacy and civil liberties” governing “the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity.”⁸ However, we are not convinced that the guidelines will overcome the problems we have identified. CISA’s broad definitions and the express purpose for federal government use of furthering Espionage Act investigations and prosecutions make it hard to envision how protective the guidelines would be of freedom of the press and the public’s right to know. We fear that it would be a case of the fox guarding the hen house.

In sum, CISA would enable the federal government to do an end-run around the Constitution and existing privacy laws. Absent the protections found in strong judicial oversight, legal standards and prior notice requirements, federal investigators and prosecutors could easily obtain the communications records of journalists and their confidential sources, thereby creating an impermissible chilling effect on newsgathering and irreversibly harming the flow of accurate news and information to the public and policymakers.

Therefore, we ask that the Committee take a deliberate and thoughtful approach to narrowing the bill’s definitions and permitted purposes to strengthen cybersecurity without threatening the reporting of accurate news and information.

Sincerely,

Members of the Sunshine in Government Initiative

Contact: Rick Blum, Director, rblum@sunshineingovernment.org, (571) 481-9322.

CC: Sen. Patrick Leahy, Chairman, Senate Judiciary Committee
Sen. Chuck Schumer
Sen. Lindsey Graham
Sen. Harry Reid, Senate Majority Leader

⁸ Section 5(b), 5(d)(5)(C).