epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

February 28, 2018

The Honorable Elise Stefanik, Chairman
The Honorable James Langevin, Ranking Member
U.S. House Committee on Armed Services
Subcommittee on Emerging Threats and Capabilities
2216 Rayburn House Office Building
Washington, D.C. 20510

Dear Chairman Stefanik and Ranking Member Langevin:

We write to you regarding the upcoming hearing, "A Review and Assessment of the Department of Defense Budget, Strategy, Policy, and Programs for Cyber Operations and U.S. Cyber Command for Fiscal Year 2019."[1] EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] We are particularly interested in the privacy issues raised by the government's cybersecurity policies.

At the end of 2015, the Cybersecurity Act of 2015 was signed into law.[3] Title I of that act, known as the Cybersecurity Information Sharing Act of 2015 (CISA), created a mechanism for the private sector to provide cyber threat information to the federal government.[4] Much of that information concerns the activities of individual Internet users.

CISA and earlier bills, such as the Cyber Intelligence Sharing and Protection Act (CISPA), raised substantial privacy concerns.[5] With the passage of the Cybersecurity Act of 2015, the risk to privacy still remains.[6] The Department of Homeland Security (DHS) developed the Automated Indicator Sharing (AIS) initiative as the primary tool to receive and disseminate

[1] *A Review and Assessment of the Department of Defense Budget, Strategy, Policy, and Programs for Cyber Operations and U.S. Cyber Command for Fiscal Year 2019*, 115th Cong. (2018), H. Comm. on Armed Services Subcomm. on Emerging Threats and Capabilities (Feb. 28, 2018), http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=106899.
[2] *See About EPIC*, EPIC.org, https://epic.org/epic/about.html.
[3] Consolidated Appropriations Act, 2016, Public Law 114-113, December 18, 2015, 129 Stat 2242, 6 U.S.C. 1501-1510.
[4] *Id.*
[5] *See* Jeramie D. Scott, *Cybersecurity: the view from Washington*, Daily Journal (Jan. 28, 2015), *available at* https://epic.org/epic/jeramie-scott-cybersecurity-oped.pdf; Wired staff, *CISA Security Bill Passes Senate With Privacy Flaws Unfixed*, Wired (Oct. 27, 2015), https://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/.
[6] *See* Taylor Armerding, *Information Sharing Bill Passes, But Privacy Debate Goes On*, CSO (Jan. 14, 2016), https://www.csoonline.com/article/3021907/security/information-sharing-bill-passes-but-privacy-debate-goes-on.html.

cyber threat indicators and defensive measures information.[7] AIS relies on an automated analysis with minimal human review to remove personal information before the information is sent to federal agencies like the Department of Defense (DoD).[8] This information is acquired by the federal government without the privacy safeguards, such as judicial review and probable cause, that would otherwise apply under the federal wiretap statute.

Effective oversight of the government's collection of personal data is particularly important in the realm of cybersecurity where it is easy to obtain vast troves of personal data with little accountability. The history of the U.S. government's surveillance of domestic communications in collaboration with private companies[9] makes it imperative that Congress ensure that CISA safeguards Americans' privacy.

CISA requires a joint periodic audit of the actions taken by federal entities to carry out the requirements of the Act.[10] The most recent joint audit, released in December 2017, provides only the vaguest information to the public regarding the implementation of CISA.

According to the joint audit, four DoD components share or receive cyber threat indicators or defensive measures under CISA: The Office of the Chief of Information Officer and DoD Cyber Crime Center (DoD CIO and DC3), the National Security Agency (NSA), the U.S. Cyber Command (USCYBERCOM), and the Defense Information Systems Agency (DISA).[11] The audit could not assess the sufficiency of "cyber threat sharing" policies and procedures for DISA and USCYBERCOM because the DoD components did not identify any.[12] No reason is provided in the audit for why DISA and USCYBERCOM did not provide policies and procedures for the dissemination of cyber threat information.

Additionally, the DoD CIO and DC3 and USCYBERCOM, among other federal entities, stated they "took adequate steps to reduce any adverse effects" that the activities under CISA may have on privacy and civil liberties. The "adverse effects" are not detailed in the audit nor are the steps taken to remedy the issue.

We urge you to ask Admiral Michael S. Rogers detailed questions about the joint audit regarding the implementation of CISA, including:

1. Does the DISA and USCYBERCOM have policies, procedures, or guidelines for the dissemination of cyber threat information?

---

[7] The Department of Homeland Security and The Department of Justice, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015*, 8 (June 15, 2016), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_%28Sec%20105%28b%29%29.pdf.

[8] US-CERT, *Automated Indicator Sharing (AIS)*, https://www.us-cert.gov/ais.

[9] EPIC, *EPIC v. DEA*, https://epic.org/foia/dea/hemisphere/.

[10] 6 USC § 1506(b).

[11] Office of the Inspector General of the Intelligence Community, *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of* 2015, 11 n.9 (Dec. 19, 2017), https://media.defense.gov/2018/Feb/01/2001872263/-1/-1/1/AUD-2017-005.PDF.

[12] *Id.* at 12.

2. What "adverse effects" on privacy and civil liberties did DoD identify in the implementation of CISA?

3. What detailed steps did DoD take to reduce these adverse effects?

4. What are the privacy risks you see with the current mechanism to provide cyber threat information to the government?

5. What more could be done to safeguard the personal data of Americans?

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow

/s/ *Jeramie Scott*
Jeramie D. Scott
National Security Counsel