epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

February 13, 2017

The Honorable Barbara Comstock, Chair
The Honorable Eddie Bernice Johnson, Ranking Member
House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
2321 Rayburn House Office Building
Washington, DC 20515

RE: Hearing on Strengthening U.S. Cybersecurity Capabilities

Dear Chairwoman Comstock and Ranking Member Johnson:

We write to you regarding the hearing on "Strengthening U.S. Cybersecurity Capabilities" that will be held February 14, 2017. EPIC has an active interest in this effort. Weaknesses in cyber security threaten both consumers and democratic institutions.[1] EPIC is currently pursuing two Freedom of Information Act lawsuits to learn more about the Russian interference in the 2016 Presidential election.[2] EPIC filed these FOIA suits in order to understand, to the fullest extent possible, current cyber security risks to democratic institutions. We welcome your leadership on this critical issue and look forward to opportunities to work with you and your staff.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC was specifically established to advocate for the use of strong encryption technology and for the development of related Privacy Enhancing Technologies. EPIC led the effort in the United States in the 1990s to support strong encryption tools and played a key role in the development of the international framework for cryptography policy that favored the deployment of strong security measures to safeguard personal information.[4]

---

[1] *See* Democracy and Cybersecurity: Preserving Democratic Institutions, EPIC, https://epic.org/democracy/.
[2] *EPIC v. ODNI*, No. 17-163 (D.D.C. Jan. 25, 2017); *EPIC v. FBI*, No. 17-121 (D.D.C. Jan. 18, 2017).
[3] *See About EPIC*, EPIC, https://epic.org/epic/about.html.
[4] *See* Statement of EPIC President Marc Rotenberg, *The Computer Security Act of 1987 and the Memorandum of Understanding Between NIST and the NSA*, Hearing Before the U.S. House Committee on Government Operations, May 4, 1989, https://epic.org/crypto/csa/Rotenberg-Testimony-CSA-1989.pdf; Statement of EPIC President Marc Rotenberg, *Cypto Legislation*, Hearing Before the U.S. Senate Committee on Commerce, Science, and Transportation, June 26, 1996, https://epic.org/crypto/export_controls/epic_testimony_696.html.

Data protection and privacy should remain a central focus of the cyber security policy of the United States. It is precisely the extensive collection of personal information without adequate safeguards that places the United States at risk from cyber criminals and foreign adversaries. In 2015, more than 22 million records of federal employees, including 5 million digitized fingerprints and the sensitive form SF-86, were compromised. So-called "credit monitoring services" are an insufficient response to the ongoing risk to the financial records, medical records, and private communications of Americans.

Strong encryption policy and robust technical measures must be enacted in order to safeguard personal data. Weaknesses in security standards create vulnerabilities for American businesses and consumers that will be exploited by foreign adversaries. Where it is possible to minimize or eliminate the collection of personally identifiable information, the risk to the American public will be reduced.

The Cyber Security Information "Sharing" Act is now in force. That law facilitates the transfer of customer and client data from the private sector to the government, raising widespread concerns among technical experts and privacy organizations about the protection of personal information. While we favor a cooperative relationship between companies and the federal government concerning cyber security, the federal government must respect the privacy obligations of private companies and ensure the transparency of its own conduct. In the cyber security domain, as with other programs supported by taxpayer dollars, the government must uphold the law and remain open and accountable.

Finally, Congress should strengthen the federal Privacy Act. Personal data stored in federal agencies remains one of the key targets of criminal hackers and foreign adversaries. Significant steps were taken by the last administration to establish a Federal Privacy Council and to coordinate privacy protection across the federal agencies. Still, more should be done, including updates to the federal privacy law and the establishment of a data protection agency in the United States.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on Research and Technology 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