epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

January 10, 2017

Senator Ron Johnson
Senator Claire McCaskill
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill,

We write to you regarding the appointment of Thomas P. Bossert for White House Homeland Security Advisor. The position will be equal in status to the National Security Advisor. The Homeland Security Advisor will provide advice to the President regarding homeland security and counterterrorism, including cyber security.

This is an enormously important position with significant implications for the safety and security of the American people. The Homeland Security Advisor routinely briefs the President on cyber threats and directs White House policy. Although the President's Homeland Security Advisor is not subject to Senate confirmation, we urge you to work closely with Mr. Bossert (@TomBossert).

In the short term, we believe that the White House should ensure that the Russian government poses no further threats to the United States electoral system or to other democratic governments. This will require close diplomatic cooperation and a strengthening of key technical agreements. The urgency of this matter cannot be overstated. Similar cyber attacks threaten to disrupt and destabilize U.S. allies and trading partners.

Regarding his role, Mr. Bossert has stated that the United States "must work toward cyber doctrine that reflects the wisdom of free markets, private competition and the important but limited role of government in establishing and enforcing the rule of law, honoring the rights of personal property, the benefits of free and fair trade and the fundamental principles of liberty."

We are not entirely sure what that means. Certainly, the Homeland Security Advisor must help protect the safety and security of the United States and the American people. Those involved in the management of the Internet also speak of

the need to protect the "security and reliability" of the network. Unquestionably, the government must be responsible for the defense of federal agencies and government assets.

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.

The President's Homeland Security Advisor should also make clear at the outset his support for a policy of strong encryption and robust technical measures 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 President's Homeland Security Advisor should be open with the American public, as he should be with the Congress, about the current levels of cyber risk to the United States. Where it is possible, specific evidence and data should be provided to substantiate claims. Metrics that help analyze and assess risk will lead to more coherent policies across the federal government and the private sector.

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, we expect the President's Homeland Security Advisor will work with Congress to 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 look forward to working with you on these issues of vital importance to the American public.

Sincerely,

Marc Rotenberg
Marc Rotenberg,
EPIC President

Members of the EPIC Advisory Board:

Professor Ross Anderson
Professor Colin J. Bennett
Dr. David Chaum
Professor Danielle Citron
Bill Coleman
Professor Julie Cohen
Professor Laura Donohue
Professor Anna Lysyanskaya
Professor David Farber
Addison Fischer
Professor Ian Kerr
Professor Harry Lewis
Professor *emeritus* Gary Marx
Mary Minow
Professor Eben Moglen
Dr. Pablo Molina
Professor Helen Nissenbaum
Dr. Peter Neumann
Professor Frank Pasquale
Dr. Deborah Peel
Stephanie Perrin
Professor Ronald L. Rivest
Bruce Schneier
Dr. Barbara Simons
Professor Nadine Strossen
Professor Latanya Sweeney
Professor Sherry Turkle
Edward Viltz
Professor Shoshana Zuboff

Other Technology Experts:

Professor Boaz Barak
Professor David L. Dill
Dr. Joseph Lorenzo Hall
Professor Candice Hoke
Douglas W. Jones
Professor Ari Jules
Professor Steven Myers
Professor Philip B. Stark
Professor Philip Rogaway
Dr. Greg Rose
Professor James Waldo