JOHN THUNE, SOUTH DAKOTA, CHAIRMAN

ROGER WICKER, MISSISSIPPI
ROY BLUNT, MISSOURI
MARCO RUBIO, FLORIDA
KELLY AYOTTE, NEW HAMPSHIRE
TED CRUZ, TEXAS
DEB FISCHER, NEBRASKA
JERRY MORAN, KANSAS
DAN SULLIVAN, ALASKA
RON JOHNSON, WISCONSIN
DEAN HELLER, NEVADA
CORY GARDNER, COLORADO
STEVE DAINES, MONTANA

BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
CLAIRE McCASKILL, MISSOURI
AMY KLOBUCHAR, MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, HAWAII
EDWARD MARKEY, MASSACHUSETTS
CORY BOOKER, NEW JERSEY
TOM UDALL, NEW MEXICO
JOE MANCHIN III, WEST VIRGINIA
GARY PETERS, MICHIGAN

DAVID SCHWIETERT, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
WASHINGTON, DC 20510–6125
WEBSITE: http://commerce.senate.gov

April 30, 2015

The President
The White House
Washington, D.C. 20500

Dear Mr. President:

I write today to seek your assurance that recent attacks on the White House information system have not compromised the personally identifiable information of our fellow Americans, and to ensure that, if such information has been compromised, the White House will move quickly to notify the affected individuals.

Recent reports indicate that a malicious cyber intrusion[1] on the unclassified computer system of the White House, attributed to Russian hackers, is more extensive than previously known.[2] Though the hackers do not appear to have accessed any classified information, the unclassified computer system reportedly contains a great deal of sensitive information, such as schedules, policy discussions, and e-mails you sent and received, including exchanges with ambassadors.[3]

This unclassified computer system likely also contains the personally identifiable information of many Americans. In order to enter the White House complex, whether for an official business meeting, tour, or social function, an individual must submit his or her date of birth, social security number, gender, country of birth, citizenship, and place of residence. This information is often sent via e-mail, including by congressional offices relaying tour requests. I am therefore concerned that this recent incident may have exposed the personally identifiable information of many individuals and they may, as yet, be unaware of their vulnerability.

Increasing reports of attacks across Executive Branch departments and agencies raise serious questions as to whether they are adequately prepared to address vulnerabilities and protect sensitive information.[4] Given this recent hack, as well as prior incidents in 2009 and 2011,[5] concerns remain that the White House's network infrastructure remains vulnerable.

You have proposed legislation that would require companies to notify consumers when their personally identifiable information has been compromised, a goal I share as chairman of the Senate committee most directly involved with the protection of such data. You also have

---

[1] Ellen Nakashima, *Hackers breach some White House computers*, WASH. POST, Oct. 28, 2014.
[2] Michael S. Schmidt & David E. Sanger, *Russian Hackers Read Obama's Unclassified Emails, Officials Say*, N.Y. TIMES, Apr. 26, 2015, A1.
[3] *Id.*
[4] *See, e.g.*, Chris Frates & Curt Devine, *Government hacks and security breaches skyrocket*, CNN, Dec. 19, 2014.
[5] *See* Michael D. Sheer, *E-mail Outage Forces White House to Operate the Oldfangled Way*, WASH. POST; Ed O'Keefe & Anne E. Kornblut, *E-mail outage affecting the White House, OMB*, WASH. POST, Feb. 3, 2011.

identified cybersecurity as "one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter."[6] Under the Federal Information Security Management Act (FISMA), the Director of the Office of Management and Budget (OMB), within the Executive Office of the President, oversees all federal agencies' information security policies and practices and issues direction on data breach notification and implementation of the National Institute of Standards and Technology's information security standards. According to OMB's most recent government-wide FISMA assessment, Executive Branch departments and agencies continue to face serious security challenges.[7]

To allow the Committee to understand the scope of this reported breach and the steps the White House is taking to address the potential exposure of the personally identifiable information of visitors to the White House, as well as to regain the trust of the American public, please provide responses to the following questions as soon as possible, but by no later than May 15, 2015:

1. Did the recent cyber incident discussed above involve the access or loss of personally identifiable information?

2. If yes, has the White House ensured that those affected have been notified in a manner consistent with OMB policy on data breach notification, the Privacy Act, and in keeping with your own recommended direction to business entities under your data breach notification legislative proposal?

3. What steps is the White House taking to protect against similar incidents going forward?

4. What policies does the White House have in place to ensure that individuals are properly notified when their personal identifiable information has been compromised due to a breach of its information systems?

Thank you for your attention to this matter.

Sincerely,

JOHN THUNE
Chairman

cc: The Honorable Bill Nelson, Ranking Member

---

[6] The White House, Foreign Policy, The Comprehensive National Cybersecurity Initiative, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Apr. 28, 2015).
[7] Exec. Office of the President, Office of Management & Budget, *Annual Report to Congress: Federal Information Security Management Act* (Feb. 27, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.