

RON JOHNSON, WISCONSIN, CHAIRMAN

JOHN McCAIN, ARIZONA
ROB PORTMAN, OHIO
RAND PAUL, KENTUCKY
JAMES LANKFORD, OKLAHOMA
MICHAEL B. ENZI, WYOMING
KELLY AYOTTE, NEW HAMPSHIRE
JONI ERNST, IOWA
BEN SASSE, NEBRASKA

THOMAS R. CARPER, DELAWARE
CLAIRE McCASKILL, MISSOURI
JON TESTER, MONTANA
TAMMY BALDWIN, WISCONSIN
HEIDI HEITKAMP, NORTH DAKOTA
CORY A. BOOKER, NEW JERSEY
GARY C. PETERS, MICHIGAN

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

KEITH B. ASHDOWN, STAFF DIRECTOR
GABRIELLE A. BATKIN, MINORITY STAFF DIRECTOR

December 21, 2015

The Honorable Shaun Donovan
Director
The Office of Management and Budget
725 17th Street, NW
Washington, D.C. 20503

Dear Mr. Donovan:

I write to express concern regarding the dramatic rise in federal cybersecurity incidents involving private personally identifiable information (PII) and to emphasize the necessary role the Office of Management and Budget must continue to play to protect the private personal information of individuals housed on federal agency databases from internal unauthorized and illegal access.

Several instances of illegal internal access of PII data have been highlighted in the news and there is growing concern about material, government-wide vulnerabilities to internal information security threats. A November 2015 Social Security Administration Inspector General report revealed that no fewer than 50 employees internally accessed protected data without authorization.¹ The Senate Homeland Security Committee received testimony this year that a Veterans Affairs whistleblower was subjected to retaliation by other agency employees who illegally and improperly accessed his private medical records.² These incidents, among many other reported and unreported examples, help to flesh out the real and increasing challenges we face.

On November 17, 2015, I co-chaired a bicameral hearing on the widespread internal unauthorized access and dissemination of Congressman Jason Chaffetz's protected records by 45 employees at the U.S. Secret Service. At the hearing the Government Accountability Office (GAO) provided alarming testimony revealing that not one federal agency could serve as a "model agency" for how agencies should protect PII from internal intrusions.

Since 1997, GAO has designated federal information security as a federal high-risk area, and in February 2015 they updated their high-risk list to include protecting PII. In a separate

¹ OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMIN., *Audit Report: Social Security Administration Employees with Conduct Issues Who Received Monetary Awards*, A-08-15-50020, at 4-5 (November 2, 2015).

² U.S. SENATE. Comm. on Homeland Security and Gov't Affairs. *Hearing on Improving VA Accountability: Examining First-Hand Accounts of Department of Veterans Affairs Whistleblowers*. Sept. 22, 2015. 114th Cong. (statement of Brandon W. Coleman Sr., Addiction Therapist, Phoenix Veterans Affairs Health Care System).

information security report from July 8, 2015, GAO found that increased cybersecurity threats present significant challenges for agencies to mitigate. Concerning PII, this report reflects that in 2013 “eight federal agencies had inconsistently implemented policies and procedures for responding to data breaches involving PII.” The report also noted that “OMB requirements for reporting PII-related data breaches were not always feasible or necessary” and that OMB should “revise its guidance to agencies on responding to a PII-related data breach.”³

The E-Government Act of 2002 established the Chief Information Officers Council (the Council), which is chaired by OMB’s Deputy Director for Management. In practice, the Federal Chief Information Officer is the Director of the Council and leads its activities. The Council is required to “develop recommendations on information technology standards...and guidelines for Federal Government computer system efficiency and security.”⁴ According to GAO⁵, the Federal Information Security Modernization Act of 2014 (FISMA)⁶ also requires OMB to:

- Maintain oversight responsibilities of information security programs;
- Include in its annual report to Congress a summary of major agency information security incidents, an assessment of agency compliance with NIST standards, and an assessment of agency compliance with breach notification requirements;
- (For two years after enactment) Include in its annual report an assessment of agencies’ adoption of continuous diagnostic technologies and other advanced security tools;
- Update data breach notification policies and guidelines periodically and require notice to congressional committees and affected individuals; and
- (In consultation with DHS, the Chief Information Officers Council, the Council of Inspectors General on Integrity and Efficiency, and other interested parties as appropriate) Ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

It is clear that the internal protection of PII remains a serious challenge and OMB must lead by developing stronger federal information technology guidelines and protections for agencies to institute and follow. Strong federal information technology security protections are critical to safeguard the data of millions of Americans and I urge OMB to lead the way with the necessary proactive solutions to preclude future internal threats to agency systems.

³ *Id.* at 12.

⁴ E-Government Act of 2002, 44 U.S.C. 101 § 3603, *et seq.*

⁵ U.S. GOV’T ACCOUNTABILITY OFFICE, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15- 714 at 9-10 (Sept. 29, 2015).

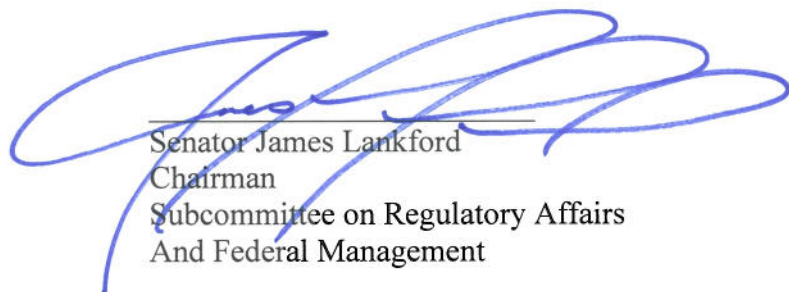
⁶ Pub. Law No. 113–283.

Based on the forgoing, I would like to request information and pertinent documents concerning the following questions as soon as possible but no later than 5:00 p.m., January 18, 2016.

- Given the increase in data of ordinary Americans collected by various federal entities, does OMB track the number incidents which involve the internal unauthorized access of PII? If yes, then please explain what OMB does with that information.
- Please provide all guidance or memos from January 1, 2010 to March 25, 2015, regarding the internal unauthorized access of PII OMB has provided for agencies prior to the Secret Service incidents of March 25, 2015.
- If OMB has not issued any guidance regarding the issue of unauthorized internal accesses of federal government databases by individuals who have credentials to access them, then does OMB intend to address this issue? If this answer is yes then please provide how you intend to address this and when.
- Please provide examples, if any, of successful agency processes to restrict PII from unauthorized access from internal intrusions.
- How does OMB measure the effectiveness of agency processes to ensure they are adequately protecting PII data from internal intrusions?

Thank you for your attention to this important matter. Please deliver your responses to the RAFM Majority Staff in Room 601 of the Hart Senate Office Building and the RAFM Minority Staff in Room 605 of the Hart Senate Office Building. The Subcommittee prefers to receive all documents in electronic format. If you have any questions, please contact John Cuaderes with the Subcommittee staff at (202) 224-6704.

Sincerely,



Senator James Lankford
Chairman
Subcommittee on Regulatory Affairs
And Federal Management

cc: The Honorable Heidi Heitkamp
Ranking Member