United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

February 6, 2025

Charles Ezell
Acting Director
Office of Personnel Management
1900 E Street, N.W.
Washington, D.C. 20415

Dear Acting Director Ezell:

On January 23, 2025, federal employees began receiving mass email messages from "HR[@]opm[.]gov," reportedly a test of a new Office of Personnel Management (OPM) capability to message all federal employees. This new capability, like other OPM services, must clearly and publicly demonstrate its compliance with established law and guidance for privacy, cybersecurity, and the management of risks. Our laws set clear privacy protections and cybersecurity requirements, and I am concerned that these statutory requirements have not been met in this case. The cybersecurity concerns of these new systems are not hypothetical – employees of the National Oceanic and Atmospheric Administration (NOAA) and other agencies have already received spam emails or been signed up for newsletters they never requested, and cybersecurity researchers have already demonstrated publicly that these servers are not adequately defended. Improperly securing our federal systems presents unacceptable national security risks as we have learned through cyberattacks in previous years, including China's hack of the personal information of more than 20 million federal workers and job applicants from OPM itself. I urge you to immediately pause all activity of the "HR[@]opm[.]gov" and related servers, complete a third-party audit of the systems for potential malicious activity, and provide the information I request below, by February 20, 2025.

Federal agencies, like OPM, have been the persistent target of foreign adversaries, cybercriminals, and so-called hacktivists for over 10 years. Due to the significant threat agencies face, Congress requires all agencies to take various measures to protect the privacy of Personally Identifiable Information (PII), mitigate risks to systems, and protect the security of government data through the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Information Security Modernization Act, among other laws. OPM, however, has not indicated this new capability has undergone the required assessments for any federal system that collects or maintains PII, nor does it seem to meet federal agency cybersecurity requirements under the Federal Information Security Modernization Act (FISMA), the Cybersecurity Act of 2015, and other OMB guidance to federal agencies. Congress and previous administrations, including President Trump, recognized that these cybersecurity and privacy requirements were important to prevent Americans' data from being stolen by malicious actors and preventing significant cyber incidents with serious national security consequences. By hastily setting up the server and email and ignoring requirements and regulations, OPM has invited foreign adversaries and cybercriminals into the agency's networks and databases and damaged trust in the agency rebuilt after the 2013 hacks.

In response to these urgent concerns and request to halt all activity of the "HR[@]opm[.]gov," I am requesting that you respond to the following questions by February 20, 2025, to clarify how you are protecting the privacy and security of government data:

1. Please describe the reason OPM set up the server and initiated the mass emails to employees.
2. Please identify the person who directed the setup of the server. Please identify the person who directed the sending of mass emails.
3. Please identify the names of any individuals who are not government employees, who contributed to this server.
4. Please identify and list any funds available to OMB and OPM that were used to purchase and set up the server for the mass emails and where the server was procured from.
5. Did OPM contract out any of this work? If so, please detail the company, or companies, used to perform any part of this work on behalf of OPM.
6. Please describe OPM's current process and policies for initiating Information Technology (IT) services such as setting up a new server for email.
7. Did setting up the new server and email require "authority to operate"? Please explain why this new server and email did or did not require "authority to operate."
8. Please provide any and all documents related to a request for an "authority to operate." Including any documentation on this activity's alignment with NIST CSF, and compliance with NIST SP 800-39, 800-37, 800-63 and other relevant guidance.
9. Please describe any and all data collected beginning January 23, 2025. Is it solely federal employee emails or data related to federal employees? What other data is being collected?
10. Where did OPM receive the list of federal employee emails or other information? Is OPM currently maintaining and updating a list of federal employee emails? Can current federal employees "opt-out" of their information being requested, maintained, updated, or otherwise used by OPM for the purposes of these mass emails? If so, where are these processes documented and how are they being made available to federal employees? Did this activity require a System of Records Notice (SORN)?
11. Based on current OPM policies and procedures for handling PII, describe the steps you are taking to mitigate privacy risks.
12. How is the collected data being accessed, shared or transmitted within OPM? Please provide documentation of risk mitigation and compliance with NIST and OMB guidance.
13. Please identify and list any data being accessed, shared or transmitted outside OPM. Please identify and list any and all agency or non-federal entity which receives or accesses the data.
14. Please provide documentation of risk mitigation and compliance with NIST and OMB guidance.
15. Please provide the names, titles, and hiring authorities of all individuals who have access to this data. Please indicate any individuals or entities, which are not government employees or bodies, that have access to this data.
16. Please provide the Privacy Threshold Analysis, Privacy Impact Assessment, or AND other privacy guidance documentation associated with this system.
17. Are you matching any data across agencies? If so, what data?
18. Are you carrying out any matching activities? If so, please provide matching agreements and documentation that those agreements have been approved by all the relevant Data Integrity Boards.
19. Do you intend to carry out any matching activities with this data that you have or will collect? If so, do you have matching agreements and have those agreements been approved by Data Integrity Boards?

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV (k)(2)(B) of the Standing Rules of the Senate to investigate matters that aid the Committee in "studying the efficiency, economy, and effectiveness of all agencies and departments of the Government." Under Senate Resolution 59, Sec. 12(e)(2), of the 118th Congress, the Committee's investigative duties "shall not be construed to be limited to the records, functions and operations of any particular branch of the Government and may extend to the records and activities of any persons, corporation, or other entity."

It is critical that OPM's work protects the rights of all its employees and that the government maintain the integrity of its data systems. The Department's work should remain non-partisan, transparent, and responsive to congressional oversight and the American people.

Thank you for your attention to this important matter.

Sincerely,

Gary C. Peters
Ranking Member
Homeland Security and
Governmental Affairs Committee