JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED NINETEENTH CONGRESS

GERALD E. CONNOLLY, VIRGINIA
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
https://oversight.house.gov

February 04, 2025

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

Dear Mr. Ezell:

We write concerning numerous reports that a server of unknown nature and origin was brought into the Office of Personnel Management (OPM) last week, connected to federal government networks, and used to access sensitive government data without regard for crucial security and privacy protections.

On January 24, 2025, millions of federal employees received an email from a new email address, hr@opm.gov, stating that it was a "test of a new distribution and response list."[1] The email address sent several additional tests before sending a mass email to the federal workforce with the subject "Fork in the Road" detailing a potentially illegal resignation offer for federal employees[2]

Just several days prior to the first test, OPM did not have the capability to email a distribution list of this scale. Acquiring such a capability securely and in compliance with federal cybersecurity, privacy, and procurement laws would likely not have been possible in such a short timeframe.[3]

Compounding our concerns, other reports suggest that allies of Elon Musk recently installed at OPM have revoked senior career employee access to OPM computer systems containing extremely sensitive information, including the dates of birth, Social Security numbers, home addresses, pay grades, and appraisals of millions of government workers. One such career

---

[1] *Trump Administration Testing System to Message All Federal Workers*, ABC News (Jan. 24, 2025) (online at https://abcnews.go.com/Politics/trump-administration-testing-system-message-federal-workers/story?id=118085501).

[2] *Id*; *Stay in Your Lane: Judiciary Rebukes Trump Admin for Email Blast to Court Employees*, Talking Points Memo (Jan. 24, 2025) (online at https://talkingpointsmemo.com/news/stay-in-your-lane-judiciary-rebukes-trump-admin-for-email-blast-to-court-employees).

[3] *OPM's New Email System Sparks Questions about Cyber Compliance*, NextGov (Jan. 28, 2025) (online at www.nextgov.com/digital-government/2025/01/opms-new-email-system-sparks-questions-about-cyber-compliance/402555/).

employee reportedly stated, "We have no visibility into what they are doing with the computer and data systems," and "There is no oversight. It creates real cybersecurity and hacking implications."[4]

The lack of security and oversight associated with the new email system and data management practices threatens to expose federal workers to personalized social engineering or "spear phishing" attacks to gain access to government systems. For example, it appears the effort to distribute the mass "Fork in the Road" email may have subverted cybersecurity controls in the National Oceanic and Atmospheric Administration (NOAA) email system leading to the agency's 13,000 employees receiving a flood of inappropriate and spam email.[5]

Additionally, the creation of a governmentwide employee database without a Privacy Impact Assessment, which conveys how personally identifiable information is collected, used, shared, and maintained, would be a dangerous violation of the 2002 E-Government Act and create a one stop shop for adversaries and nefarious actors to steal federal workers' sensitive data.[6] Furthermore, the databases that OPM used to create such a list could contain sensitive health, income, and retirement data, amplifying the risk of misuse in the wrong hands.

At best, the Trump Administration's actions at OPM to date demonstrate gross negligence, severe incompetence, and a chaotic disregard for the security of our government data and the countless services it enables our agencies to provide to the public. At worst, we fear that Trump Administration officials know full well that their actions threaten to break our government and put our citizens at risk of foreign adversaries like China and Russia gaining access to our sensitive data.

To determine the severity of reported cybersecurity and privacy violations, we are asking for responses to the following questions and requests, as well as a briefing from the Acting OPM Director and Chief of Staff, by February 18, 2025:

1. Please provide a list of any information technology equipment installed at OPM between January 21, 2025, and January 24, 2025, and used to support the distribution of the "Fork in the Road" emails, including:

    a. a description of how such equipment was procured;

    b. the associated Privacy Impact Assessment(s);

    c. the associated Authorization(s) to Operate; and

---

[4] *Exclusive: Musk Aides Lock Workers Out of OPM Computer Systems*, Reuters (Feb. 2, 2025) (online at https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/).

[5] *Trump Admin's Email System Compromised—What We Know*, Newsweek (Jan. 31, 2025) (online at www.newsweek.com/trump-noaa-email-system-compromised-2024152).

[6] Office of Management and Budget, *Request for Information: Privacy Impact Assessments* (89 Fed. Reg. 5945) (Jan. 30, 2024).

d. a list of the individuals who installed and/or accessed the equipment, including whether they were OPM employees at the time of their installation/access of the equipment and, if so:

    i. under what authority they were hired; and

    ii. what background investigation and clearance processes they underwent as part of the hiring process.

2. A list of all individuals involved in both the policy decisions and technical planning associated with any installation of new information technology equipment at OPM, the creation of the hr@opm.gov email, or the creation and distribution of the "Fork in the Road" emails, referred to hereafter as "the initiative."

3. From what databases and repositories were the "test" and "deferred resignation" email lists pulled?

4. What steps were taken to safeguard the privacy of the millions of federal employees included in those databases and repositories?

5. What IT assets, software systems, code, or other tools did the relevant team employ to collect contact information and emails for the initiative?

6. Did OPM consult with the Cybersecurity and Infrastructure Security Agency as part of the design or implementation of the initiative?

7. Has any federal employee contact information or personal information been moved, copied, or in any way distributed to IT systems outside of the federal government network as part of the initiative?

8. Did any federal government data travel outside the boundaries of the U.S. as part of the initiative?

We also request that you retain the following records and produce them to the Committee on Oversight and Government Reform staff by February 14, 2025:

1. All records, logs, code, certificates, and configurations for all IT assets that OPM used for the initiative;

2. All emails, documents, and communications relevant to the planning and execution of the initiative;

3. Any communications or records of coordination with groups outside of the U.S. government related to the initiative; and

4. All documents related to the vetting of the individuals involved in the initiative.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X. The Committee also has legislative jurisdiction over federal personnel and federal information systems. Full compliance with our requests is necessary, in part to determine whether legislative reforms are needed to ensure the continued security of our federal government systems and privacy of federal employees' sensitive personnel data. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051. Thank you for your prompt attention to this matter.

Sincerely,

Gerald E. Connolly
Ranking Member

Shontel Brown
Ranking Member
Subcommittee on Cybersecurity,
Information Technology, and
Government Innovation

cc: The Honorable James Comer, Chairman
The Honorable Nancy Mace, Chairwoman, Subcommittee on Cybersecurity, Information Technology, and Government Innovation