JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED NINETEENTH CONGRESS

ROBERT GARCIA, CALIFORNIA
RANKING 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

August 8, 2025

The Honorable Scott Kupor
Director
Office of Personnel Management
1900 E Street, NW
Washington, DC 20415

Dear Director Kupor:

Committee Democrats have obtained whistleblower evidence suggesting that Trump Administration employees installed by Elon Musk as part of his Department of Government Efficiency (DOGE) effort may have sent highly sensitive federal data, passwords, and code from your agency to unknown servers outside of the government network.[1] We have also received information indicating that DOGE has employed several foreign nationals who may have inappropriate and unlawful access to highly sensitive government data.[2] These revelations add to our continuing alarm that members of DOGE are acting with broad disregard for the security of Americans' data, endangering sensitive information and putting our national security at risk. We request that the Office of Personnel Management (OPM) provide an immediate briefing on the evidence enclosed with this letter, including whether OPM leadership was aware of the potential exfiltration of code and credentials, the potential threat of a breach of sensitive government personnel data, and the additional requested information and documents needed to assess potential threats to the American people.

Committee Democrats recently received evidence that DOGE staff inside OPM had sent a specific type of highly sensitive electronic files to internet protocol (IP) addresses outside of the federal government.[3] These files, known as Docker images, can include the information and keys needed to remotely access government applications and databases. Docker images are bundles that contain everything needed to run an application, including code, settings, and sometimes sensitive information like security keys and login credentials.[4] Once a Docker image

---

[1] Communications with Committee Democratic Staff.

[2] Communications with Committee Democratic Staff; Letter from Ranking Member Gerald E. Connolly, Committee on Oversight and Government Reform, to Mr. David Warrington, Counsel to the President (Jan. 30, 2025) (online at https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025.01.30.%20GEC%20to%20WH%20Counsel%20-%20EOP%20Clearances.pdf).

[3] *See* WhoIs RIPE Database records for IP addresses in range 172.128.0.0 - 172.215.255.255, 20.192.0.0 - 20.255.255.255.

[4] *What is Docker*, DockerDocs (online at https://docs.docker.com/get-started/docker-overview/) (accessed June 18, 2025).

leaves the protection of government networks, anyone who gets a copy could potentially use it to access federal systems and databases without authorization, putting sensitive data at serious risk. For example, private actors or adversarial governments could potentially use this information to log into databases that hold sensitive data and could do so without any indication of compromise, hiding the severity of the security breach.[5]

The obtained evidence suggests that DOGE staff potentially stole these Docker images by sending them to servers outside the government network through the system OPM uses to install new updates to its online retirement benefits portal for federal employees, known as OPM's Online Retirement Application (ORA).[6] This system serves as a gateway for civil servants to access their benefits upon retirement and includes their personally identifiable information. There is no reason that Docker images—which could hold the code, settings, and access credentials for the retirement system—or any other sensitive information related to the system should leave government networks. External access to this data could compromise the financial information and personal privacy of every federal employee, past and present, of both Democratic and Republican administrations.

Adding to our concern regarding DOGE's access to this highly sensitive data is the fact that Committee Democrats have received additional information indicating that several DOGE employees are foreign nationals who have received security clearances despite the fact that foreign nationals generally "do not qualify for a security clearance."[7] While foreign nationals may receive Limited Access Authorization for Secret level materials, we question the justification for granting these specific foreign nationals this special authorization to access the classified information held by OPM, rather than limiting such access to U.S. citizens who can appropriately obtain a full security clearance.[8] Given the Trump Administration's cavalier disregard for security clearances, as demonstrated by its willingness to bypass the vetting process for the highest level of government clearance for specific individuals identified by the White House Counsel, it is critical that we know which foreign nationals have been granted access to sensitive and classified information at OPM and why.[9]

This is just the latest apparent incident in the Trump Administration's history of technological incompetence and repeated failures to protect the federal government's critical

---

[5] Communications with Committee Democratic Staff.

[6] OPM's Online Retirement Application processes retirement information for federal employees and provides them with a portal to access their benefits in the Civil Service Retirement System (CSRS) and Federal Employees Retirement System (FERS). Office of Personnel Management, *Online Retirement Application (ORA) Help* (online at retire.opm.gov/help) (accessed June 6, 2025).

[7] Communications with Committee Democratic Staff; Defense Counterintelligence and Security Agency, *Security Assurances for Personnel & Facilities* (online at www.dcsa.mil/Industrial-Security/International-Programs/Security-Assurances-for-Personnel-Facilities/) (accessed June 16, 2025).

[8] *Id.*

[9] Letter from Ranking Member Gerald E. Connolly, Committee on Oversight and Government Reform, to David Warrington, Counsel to the President (Jan. 30, 2025) (online at https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025.01.30.%20GEC%20to%20WH%20Counsel%20-%20EOP%20Clearances.pdf).

information technology (IT), threatening the security of the American people's data. In February 2025, then-Oversight Committee Ranking Member Gerald E. Connolly and Cybersecurity, Information Technology, and Government Innovation Subcommittee Ranking Member Shontel Brown wrote to you regarding DOGE's provision and use of an unsecured server to send the legally questionable "Fork in the Road" email to federal employees.[10] OPM has continued to engage in irresponsible cyber and operational security practices that put federal employees' personal and financial data at risk and endanger national security.[11] DOGE's reckless approach to safeguarding sensitive data combined with these newest revelations about data exfiltration at OPM create a concerning pattern that constitutes gross negligence with regards to federal cybersecurity and risks opening federal systems to attacks from malign actors.

To understand what sensitive federal information may have been compromised and the associated risks to the American people, we request a comprehensive briefing on the enclosed evidence and the following information and documents by August 22, 2025, as well as fulsome and complete answers to our prior letters, including the one sent on February 4, 2025:

1. All logs, communications, builds, and memoranda of understanding associated with any deployments, replications, transmission, or distribution of code, containers, Docker images, and credentials associated with the ORA application at OPM from January 1, 2025, to present;

2. A list of all individuals who accessed to or had the ability to access the code and deployment pipelines for the OPM ORA application from January 1, 2025, to present; and

3. A list of all foreign nationals who have worked on OPM IT systems, including but not limited to ORA, from January 1, 2025, to present.

---

[10] Letter from Ranking Member Gerald E. Connolly, Committee on Oversight and Government Reform, and Ranking Member Shontel Brown, Subcommittee on Cybersecurity, Information Technology, and Government Innovation, to Charles Ezell, Acting Director, Office of Personnel Management (Feb. 4, 2025) (online at https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025.02.04.%20GEC%20and%20Brown%20to%20OPM-Ezell-%20DOGE%20Emails.pdf).

[11] *See* Letter from Ranking Member Gerald E. Connolly, Committee on Oversight and Government Reform, and Ranking Member Shontel Brown, Subcommittee on Cybersecurity, Information Technology, and Government Innovation, and Ranking Member Melanie Stansbury, Subcommittee on Delivering on Government Efficiency, to President Donald J. Trump (Feb. 25, 2025) (online at https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025-02-25.%20GEC%20Brown%20Stansbury%20to%20President%20Trump%20re.%20DOGE%20Cyber%20Issues.pdf); Letter from Ranking Member Gerald E. Connolly, Committee on Oversight and Government Reform, to Mr. Charles Ezell, Acting Director, Office of Personnel Management (Feb. 22, 2025) (online at https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025-02-22.GEC%20to%20OPM-%20Ezell%20re%20Musk%20Email.pdf); Letter from Ranking Member Gerald E. Connolly, Committee on Oversight and Government Reform, to Mr. Charles Ezell, Acting Director, Office of Personnel Management (Feb. 25, 2025) (online at https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025-2-25.GEC%20to%20OPM-Ezell%20-%20CIO%20SES%20Clean.pdf).

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 the privacy of sensitive federal 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,

Robert Garcia
Ranking Member

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

Enclosure

cc: The Honorable James Comer, Chairman

The Honorable Nancy Mace, Chairwoman
Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Norbert E. Vint, Deputy Inspector General, Office of Personnel Management Office of the Inspector General

CYBERSECURITY BREACH INCIDENT REPORT
PREPARED BY THE DEMOCRATIC STAFF OF THE
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

ISSUES SUMMARY: DOGE operatives at the Office of Personnel Management (OPM) sent sensitive information to servers potentially outside of the government network.

I. BACKGROUND

Committee Democrats have obtained whistleblower evidence demonstrating that DOGE staff operating inside OPM may have escalated their activities from utilizing unsecured servers to communicate with federal employees, to now actively exporting data, code, and deployment infrastructure to servers outside of federal government networks. The evidence shows that on June 2, 2025, an unidentified individual used the systems through which OPM installs new updates to its Online Retirement Application (ORA) (found at retire.opm.gov/portal) to send Docker images to unknown internet protocol (IP) addresses, suggesting that such IP addresses belong to servers outside of the federal government. The whistleblower has alleged, based on firsthand experience, that the unidentified individual was a DOGE employee. Private actors or adversarial governments could potentially use information in these docker images to log into OPM databases or servers that hold sensitive data about federal employees and could do so without any indication of compromise—hiding the severity of the incursion.[1]

II. AREAS OF COMPROMISE

Committee Democrats have documentary proof that one or multiple employees used an account that resolved as an anonymous user to deploy various applications to IP addresses that did not resolve to the typical proget.opm.gov Domain Name System (DNS) name. Discussions with individuals familiar with the development security operations (DevSecOps) systems at OPM indicated that this behavior would only occur if the deployment IP addresses existed outside of OPM's network.

III. DOCKER IMAGE LIBRARIES

A. Projects deployed to unresolved IP addresses: ora-web-production-frontend, ora-web-backend, ora-web-development-frontend, ora-web-development-backend, ora-web-production-backend, ora-web-test-frontend, ora-web-production-frontend, ora-web-development-frontend, ora-web-staging-backend, ora-web-test-backend, rs-ora-web

B. Sample IP Addresses:

172.183.230.17
172.178.111.144
20.246.79.26
51.8.152.193
20.42.51.159
172.183.230.18
52.234.42.245

[1] Communications with Committee Democratic Staff.

20.25.192.250
20.42.44.113

IV. CONCERNS OF COMPROMISE

If, as Committee Democrats were told, these docker images were distributed outside of the government, they could include code, credentials, and ssh keys or similar information that could compromise the underlying applications, databases, and OPM network more broadly. Security software would also have difficulty detecting an intrusion, as the attacker would be using the system user's legitimate credentials.

V. AREAS FOR INVESTIGATION

- Under what circumstances can an OPM engineer deploy applications with a username that resolves to "anonymous"?
- Under what circumstances can an OPM engineer user deploy applications to servers without a resolved DNS name using the deployment application?
- Are any of the sample IP addresses associated with government entities?
- Who deployed the applications as the anonymous user?
- What servers (including the users with access to those servers) did OPM deploy these applications to?
- What code, credentials, database keys, ssh keys or other data are included in the Docker images for the listed projects?

For additional information, please contact Committee Democratic staff at (202) 225-5051.