United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

February 25, 2026

Frank Bisignano
Commissioner
Social Security Administration
2100 M Street NW
Washington D.C. 20037

Dear Commissioner Bisignano:

I write to request additional information following concerning disclosures by the Department of Justice (DOJ) in *AFSCME v. SSA* as well as multiple whistleblowers and to call on you to shut down all Department of Government Efficiency (DOGE) activities, suspend all DOGE personnel, and revoke any and all of DOGE's access to Social Security Administration (SSA) data.[1] I also write to request that you address these allegations and disclosures publicly and comprehensively, and that you provide documentation to show that SSA is in compliance with applicable privacy and data security laws to ensure that the American public's data is secure.

Through a recent DOJ filing in federal court, SSA now admits that it has identified actions by the SSA DOGE Team that were likely inconsistent with SSA policy, were non-compliant with the March 20, 2025 temporary restraining order (TRO), and may have violated multiple laws. According to a recent DOJ filing in *AFSCME v. SSA*, SSA determined that prior to the TRO, a member of the SSA DOGE Team sent sensitive SSA data to Steve Davis, a DOGE colleague at the Department of Labor (DOL), and the Department of Homeland Security (DHS). SSA, while unable to access this file and verify its contents, believes it contained personally identifiable information (PII) derived from SSA systems for approximately 1,100 people. The court filing also states that SSA uncovered communications between SSA's DOGE Team and a private partisan political advocacy group seeking to compare SSA data against state voter rolls to find evidence of voter fraud and to "overturn election results in certain states." Further, a DOGE Team member signed and executed a "Voter Data Agreement" with this advocacy group that was not reviewed or approved by the proper SSA authorities.

A recent HSGAC minority report also described SSA whistleblower disclosures alleging that DOGE-affiliated employees at the agency were granted permission to upload personal data on all Americans, including Social Security numbers (SSNs), to a cloud environment without any verified security controls or standard agency visibility into their use of that data.[2] An internal SSA risk assessment of this DOGE-initiated project determined that the likelihood of a data breach with "catastrophic adverse effect" is between 35 and 65 percent.[3]

The DOJ filing makes these allegations all the more alarming. The management of sensitive agency data in compliance with federal laws, agency guidance, and other guardrails is critically important, both to safeguard

[1] *American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration*, No. 1:25-cv-00596, (D. Md. April 17, 2025)(notice by Social Security Administration of corrections to the record).

[2] Senate Committee on Homeland Security and Governmental Affairs Minority Report, *Unchecked and Unaccountable: How DOGE Jeopardizes Americans' Data Without Regard for Law and Congress* (Sept. 2025).

[3] *Id.*

vital programs like Social Security and Medicare and to protect the American public from identity theft and breaches of their most sensitive personal information. At a minimum, the DOJ filing suggests that SSA failed to adequately oversee DOGE activities and compromised sensitive personal data—precisely what the HSGAC Minority report and whistleblowers warned against. At worst, SSA was complicit in the apparent Hatch Act and Privacy Act violations and lied to Congressional investigators.

As SSA Commissioner, you have a responsibility to ensure Americans' most sensitive information that is held by SSA is safeguarded. While you have provided some additional information to Congress regarding whistleblower disclosures and DOGE oversight, you have provided incomplete or misleading answers to questions in writing and notably have not released information needed to ensure critical data is no longer at risk. Given the gravity of the admissions in the court filing, as well as prior whistleblower disclosures, I call on you to immediately halt all DOGE work and data access at SSA; conduct a thorough review of the security of SSA datasets in any cloud environment, including Cloudflare; and track down any data that was inappropriately shared outside the agency by DOGE. I urge you to expeditiously comply with these requests and refer matters, as appropriate, to the Department of Justice to ensure compliance with the Privacy Act, FISMA, the E-Government Act, and other relevant privacy and cybersecurity statutes.

Please respond to the following questions and requests no later than April 1, 2026:

1. Please provide a copy of the March 3, 2025 email from the SSA DOGE Team that copied Steve Davis, a DOGE-affiliated employee at the DOL, and DHS. Please identify the DOGE-affiliated individuals sending or receiving this email.

2. Please provide a copy of the "Voter Data Agreement" that an SSA DOGE Team member signed with the political advocacy group in March 2025 and include identification of the advocacy group. Please identify:
    a. Whether and what information or data was shared outside of SSA;
    b. Any individual, including any DOGE-affiliated individual(s), who signed or were aware of this agreement; and
    c. Any other data sharing agreements with outside groups and any individual(s) who signed such agreements, including any individuals who were detailed to SSA.
    d. List the employment status of all individuals involved in this incident or identified in response to 2(c), including all current or former DOGE-affiliated personnel.

3. Please provide additional documentation and materials related to the November 2025 review that led to the discovery of these incidents:
    a. Why did SSA initiate a review of DOGE activities in November 2025, and who at SSA was tasked with leading the review?
    b. What are the findings of that review and did SSA identify any additional actions that potentially violated the law? What actions, including disciplinary actions, resulted from that review?
    c. Who at SSA was aware of these incidents prior to November 2025?

4. Please provide copies of the referrals made to the U.S. Office of Special Counsel related to the incidents described in Section V of the DOJ filing.

5. Why is SSA unable to access the data that was shared in the March 3 email to Steve Davis and others, and why is SSA unable to investigate and determine which data were shared using Cloudflare? Why is SSA unable to determine whether the data still exists on the third-party server?
    a. How is it possible that SSA data were shared on a non-approved third-party server by DOGE without any SSA employees being aware or having access and without creating a log of associated activities?

b. Are the DOGE-affiliated individuals – including individuals who may no longer be at SSA – involved cooperating with SSA requests for access and information?

6. What investigation or audit has occurred regarding the sharing of data through third-party servers or to third parties through existing systems?

7. What work has been performed to address the usage of links to share SSA data in unapproved repositories or third-party servers? Is SSA conducting an audit or investigation to ensure no other data was shared through other means?

8. Is SSA considering this incident a data breach? If so, did SSA follow OMB guidelines for reporting the breach?[4]

9. Please provide all records referring or related to consideration of any request to transfer NUMIDENT data to a new cloud environment involving John Solly, Edward Coristine, Aram Moghaddassi, or Mike Russo since January 20, 2025, including without limitation:
    a. Risk assessments, and all records related to each assessment.
    b. Emails, text messages, Signal messages, Microsoft Teams messages, and other internal electronic communications.
    c. Any other SSA memoranda, analysis, or assessment (internal or external) related to the decision process and authorization for this request.
    d. Any related privacy threshold assessments or privacy impact assessments, and all records relating to each assessment.
    e. Any specific authorization to operate documentation, and all records associated with such documentation.
    f. Any planned future work on the project.

10. By no later than April 1, 2026, please make the following individuals available for interviews with the Committee:
    a. All DOGE-affiliated personnel assigned to SSA, including those who have since become full time employees of SSA.
    b. All employees onboarded after January 20, 2025 who appear in System Access Manager (SAM) logs for the NUMIDENT transfer project initiated by John Solly.
    c. All individuals implicated in the whistleblower disclosure and DOJ court filing (notice of corrections), as well as all SSA employees supervising those individuals.

11. Please provide all records, logs, or other documentation of activity related to any cloud environment created, utilized, or in development pursuant to any request involving John Solly, Edward Coristine, Aram Moghaddassi, or Mike Russo for the transfer of NUMIDENT or other sensitive data to that cloud environment, including:
    a. Amazon Web Service (AWS) cost and usage reports and S3 transfer metrics showing data volume movements involving NUMIDENT-sourced data between buckets;
    b. System outage logs related to NUMIDENT or systems that access NUMIDENT;
    c. Documentation of any account creation, privilege changes, service enablement, data access, or bulk transfer or externalization of NUMIDENT, including cloud audit logs, network flow records, service access logs, and database audit logs;
    d. If an edge provider such as Cloudflare was used, include configuration and request logs relevant to the identified AWS resources;
    e. All available access logs and access control policies for any object or database storage that stored or received NUMIDENT data for this project;

[4] *See* Office of Management and Budget, *Memorandum: Preparing for and Responding to a Breach of Personally Identifiable Information* (M-17-12) (Jan. 2017).

f. Artifacts for Eden API, any other APIs, or other executable code developed or deployed within the identified environment(s) that touch NUMIDENT or associated datasets.

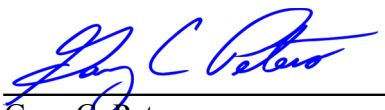
12. Please provide a detailed description of the operational need for the NUMIDENT cloud project initiated by John Solly in June 2025.
    a. Why did this operational need outweigh any potential security risks?
    b. Was this operational need related to the use of SSA data by the Department of Homeland Security, including its use of NUMIDENT data as a record source for the Systematic Alien Verification for Entitlements (SAVE) program or any other systems?
        i. If so, why were normal protocols for data sharing between agencies not followed?
        ii. If so, who at DHS has access to this data and through what mechanisms do they have access?
        iii. If DHS is using any of this data, is the NUMIDENT data point-in-time data, how is it being correlated with DHS data, and what quality assurance process is in place if any?
        iv. If the data accessed by the SAVE program, the USCIS Verification Data Integration Service, or other DHS programs are still maintained in a cloud environment, please describe the cloud environment as well as the security protections and oversight mechanisms in place.

13. Please list each individual that was granted administrative access to the cloud environment created for the NUMIDENT project initiated by John Solly in June 2025. For each individual, please provide:
    a. Documentation of any training they were provided prior to accessing this "high risk" system.
    b. Documentation of any background checks or other vetting to ensure access to sensitive data was appropriate.

14. Please provide a detailed explanation, including supporting documents and information, regarding how the data in the virtual private cloud environment was used as well as whether access was authorized to other federal, state, local, Tribal or territorial governments or private sector actors.

In addition to responding to these questions in writing, I request a briefing on this subject prior to April 1, 2026. Thank you for your attention to this letter, and I look forward to your prompt response.

Sincerely,



Gary C. Peters
United States Senator
Ranking Member, Committee on
Homeland Security and
Governmental Affairs