

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
NORTHERN DIVISION**

AMERICAN FEDERATION OF STATE,
COUNTY AND MUNICIPAL EMPLOYEES,
AFL-CIO, *et al.*,

Plaintiffs,
vs.

SOCIAL SECURITY ADMINISTRATION,
et al.,
Defendants.

Civil Action No. 1:25-cv-00596

DECLARATION OF MICHAEL L. RUSSO

I, Michael L. Russo, hereby declare upon penalty of perjury:

1. I am the Chief Information Officer of the Office of the Chief Information Officer (OCIO) at the Social Security Administration (SSA), in Woodlawn, Maryland, and I have served in this role since February 3, 2025. I am a Non-Career Senior Executive reporting directly to SSA's Acting Commissioner, Leland Dudek.
2. In my role as Chief Information Officer, I am responsible and accountable for the effective implementation of information technology (IT) management responsibilities, such as developing, maintaining, and facilitating the implementation of a sound, secure, and integrated information technology architecture for SSA. As part of my information resources management duties, I am responsible for oversight of grants of permissions to access SSA systems.
3. I provide this declaration in support of the Defendants' opposition to the Motion for a Temporary Restraining Order, Preliminary Injunction, and/or 5 U.S.C. § 705 Stay in the above-captioned case. This declaration provides information underlying the decision to

grant data access to the members of SSA's DOGE Team. These statements are made with my personal knowledge, discussion with SSA staff, and review of documents and information furnished to me in the course of my official duties.

4. Pursuant to Executive Order 14,158 ("Establishing and Implementing the President's 'Department of Government Efficiency'"), there exists within SSA a "DOGE team" responsible for "implementing the President's DOGE agenda." *Id.* § 3(c). The SSA DOGE Team currently consists of ten SSA employees: four SSA special government employees (Employees 1, 4, 6, and 9) and six detailees to SSA from other government agencies and offices (Employees 2, 3, 5, 7, 8, and 10). To protect the privacy of these individuals, and to avoid exposing them to threats and harassment, I have not listed their names in this declaration.
5. The overall goal of the work performed by SSA's DOGE Team is to detect fraud, waste and abuse in SSA programs and to provide recommendations for action to the Acting Commissioner of SSA, the SSA Office of the Inspector General, and the Executive Office of the President.
6. In the case of DOGE team data access, data access to the DOGE team was first approved by SSA's Acting Commissioner.
7. Employee 1, an SSA special government employee, was granted access to, a production copy with read-only access and no update ability, the following information on the following dates:
 - a. On February 12, 2025, access was granted to anonymized data (i.e., data that had personal identifiers removed) from SSA's Master Beneficiary Record (MBR) (System of Records Notice 60-0090), Supplemental Security Record (SSR)

(System of Records Notice 60-0103), the Master File of Social Security Number Holders and SSN Applications (also known as the Numident, System of Records Notice 60-0058), and Treasury Payment Files Showing SSA Payments (containing information from Social Security Online Accounting and Reporting System, System of Records (SSOARS) Notice 60-0231).

- b. On February 20, 2025, access was granted to personally identifiable information from copies of SSA's MBR, SSR, Numident, and Treasury Payment Files Showing SSA Payments from SSOARS.
- c. SSA MBR and SSR may contain limited fields containing information sourced from federal tax information that SSA uses in benefits eligibility calculations and determinations.
- d. Employee 1 needs access to the personally identifiable information and limited tax return information in the data that he was granted access to because he could not complete the work he is tasked with using anonymized versions of the data, as the analysis tasked requires an examination of individual-level benefits data, payments data, and Numident records.
- e. Employee 1 needs access to the limited federal tax information in the MBR and SSR, which is comingled with SSA's benefits records, because it is part of the benefits payment-related data. For instance, SSA uses federal tax information in calculations of earnings (often with other non-tax earnings data in SSA records) in determining benefits eligibility. Employee 1 was not granted access to SSA's separate repository of federal tax information, which is SSA's Master Earnings File (Privacy Act System of Records 60-0059).

8. On February 21, 2025, Employee 3, an SSA detailee, was granted access to, a production copy with read-only access and no update ability, personally identifiable information from SSA's MBR, SSR, Numident, and Treasury Payment Files Showing SSA Payments from SSOARS. His need for the data access granted is the same as Employee 1 (see paragraph 7.d-e).
9. On February 21, 2025, Employee 5, an SSA detailee, was granted access to, a production copy with read-only access and no update ability, personally identifiable information from SSA's MBR, SSR, Numident, and Treasury Payment Files Showing SSA Payments from SSOARS. He was granted systems access to several other databases but never accessed the data in them. His need for the data access granted is the same as Employee 1 (see paragraph 7.d-e).
10. On February 22, 2025, Employee 10, an SSA detailee, was granted access to, a production copy with read-only access and no update ability, personally identifiable information from SSA's MBR, SSR, Numident, and Treasury Payment Files Showing SSA Payments from SSOARS. His need for the data access granted is the same as Employee 1 (see paragraph 7.d-e).
11. On March 4, 2025, Employee 9, an SSA special government employee, was granted access to, a production copy with read-only access and no update ability, personally identifiable information from SSA's MBR, SSR, Numident, and Treasury Payment Files Showing SSA Payments from SSOARS. His need for the data access granted is the same as Employee 1 (see paragraph 7.d-e).
12. On March 6, 2025, Employee 8, an SSA detailee, was granted access to, a production copy with read-only access and no update ability, personally identifiable information

from SSA's MBR, SSR, Numident, and Treasury Payment Files Showing SSA Payments from SSOARS. His need for the data access granted is the same as Employee 1 (see paragraph 7.d-e).

13. Employee 2, an SSA detailee, has not received access to any SSA programmatic data or systems. He has only accessed limited personnel data about SSA workforce, provided by Human Resources. The data was used to provide some detail about the number of people affected and their respective titles by category to the Office of Personnel Management (OPM), which was conveyed in an SSA memo to OPM. This employee is acting as SSA's DOGE Team lead and as part of his duties is responsible for consulting on the agency's workforce plans, including but not limited to reorganization and hiring. These duties necessitated the need for this limited workforce data.
14. On March 11, 2025, Employee 7, an SSA detailee, was granted access to SSA systems but he has only accessed data from SSA's Numident. All other access initially granted has since been revoked pending review of further data access needs. He required access to the files because his work involves analysis of improper payments relating to death records maintained in the Numident.
15. Not on behalf of SSA, but as Health and Human Services/Office of Child Support Services (OCSS) authorized users, Employee 7 and Employee 3 were granted access as a National Directory of New Hire Data. This file is maintained on SSA's network for OCSS; we have a Service Level Agreement with OCSS describing how SSA will grant users to OCSS authorized users upon receipt of OCSS permissions. OCSS permissions were obtained prior to granting Employee 7 and Employee 3 access.

16. No SSA data or personally identifiable information access, or access to systems containing such information, has been granted to Employee 6 and Employee 4.
17. To the best of my knowledge, the data and systems listed in paragraphs 7 through 14 above contain a complete listing of all SSA data accessed by the listed SSA employees working with the DOGE Team, as of the date of this declaration.
18. There are five other individuals whose services were authorized under our interagency agreements with U.S. DOGE Service, previously U.S. Digital Service. Some of these individuals predated the creation of U.S. DOGE Service. However, the agency has determined it does not need these individuals services, these individuals were never working with the SSA DOGE Team or granted access to sensitive agency data or personally identifiable information, and SSA is in the process of terminating their arrangements with SSA.
19. In each case of data access being granted above, the agency has provided read-only access to copies of production data which does not allow modification or deletion of the underlying data. This level of access provides no access to SSA production automation, code, or configuration files, and provides no avenues to alter the function of SSA production systems. This level of access ensures these employees can review records needed to detect fraud but does not allow them the ability to make any changes to beneficiary data or payment files.
20. The data sets provided were obtained from SSA's Enterprise Data Warehouse (EDW). The EDW is an integrated source of data created to service Management Information, Business Intelligence, and predictive analytics across SSA. EDW data sets are copies of production data like those provided to the individuals identified above, are routinely used

for analytics purposes by employees performing analysis on agency data within job duties, such as anti-fraud analysis or research. SSA's Office of Financial Policy and Program Integrity confirmed the level of access granted to the DOGE team to perform analysis has similarly been granted to 30-40 SSA employees in their component.

21. The individuals above who have been granted access have all received SSA training on topics including ethics, the Privacy Act, and information security. They also have acknowledged and signed the Systems Sanctions Access Policy and Annual Reminders on Safeguarding PII. This is the same level of training that we provide our other SSA employees.

22. SSA has IT safeguards to ensure no private or commercial servers have been integrated with SSA systems. SSA performs continuous network monitoring that includes identifying unauthorized devices. The agency further has extensive security layers in place ensuring access to all systems and records are controlled and tracked with appropriate profiling (e.g., employee, contractor, supervisor) of the user.

I declare the foregoing to be true and correct, upon penalty of perjury.

Date: _____

Michael
L. Russo

Digitally signed by
Michael L. Russo
Date: 2025.03.12
15:38:37 -04'00'

Signed: _____

Michael L. Russo
Chief Information Officer
Office of the Chief Information Officer
Social Security Administration