EXHIBIT A

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

SUPPLEMENTAL DECLARATION OF ERIE MEYER

I, Erie Meyer, declare as follows:

1. I am a founding member of the U.S. Digital Service and have served as the Chief Technologist of two federal agencies. I have significant experience in technology policy, data security, and artificial intelligence.

2. I previously submitted a declaration in this matter. Everything I said in that declaration remains true. I submit this declaration to provide additional information relevant to this case.

3. According to filings from the defendants in this case, the Department of Government Efficiency ("DOGE") has requested broad access to numerous Social Security Administration ("SSA") data systems, including the Numident, Master Beneficiary Record ("MBR"), Supplemental Security Record ("SSR"), and other databases that collectively contain deeply personal information about nearly every person ever born in the United States. These records include Social Security numbers, birthdates, home addresses, employment history,

earnings, disability records, bank account information, medical documentation, and in some limited cases, classified data used to support national security.[1]

4. The access DOGE is requesting materially increases the risk of hacking and data exploitation. The SSA operates one of the most sensitive data environments in the federal government. Centralizing this information, along with a mandate to rapidly deploy AI and automation tools, introduces unprecedented cybersecurity risk. The possibility of compromise—whether through external cyberattacks or internal misuse—becomes far greater as more individuals and systems gain programmatic access to sensitive personal data.

5. Stalkers, scammers, and spies materially benefit when a group of people—particularly those who have not been subject to full vetting and data controls—are granted broad and centralized access to personally identifiable information ("PII") on nearly every American. For example, access to SSA's disability systems includes detailed psychotherapy notes, records of reproductive health, and comprehensive data about children's medical and school history. If this data were to be improperly accessed, misused, or leaked, it could cause irreparable harm to the privacy, safety, and dignity of vulnerable individuals, including children, veterans, and survivors of domestic violence, and open them up to economic exploitation.

6. Security research and prior incidents have shown that once a system with broad access to sensitive information is compromised, it is nearly impossible to contain the damage. Threat actors, whether criminal organizations, hostile nation-states, or malicious insiders, routinely seek access to government databases. By consolidating access to all of SSA's systems with aggressive timelines and AI ambitions, the risk is exponentially compounded.[2]

[1] Jacob Leibenluft et al., *Trump Administration, DOGE Activities Risk SSA Operations and Security of Personal Data*, Ctr. on Budget and Policy Priorities 18 (April 1, 2025), https://perma.cc/EM5E-GPUZ.
[2] *Id.* at 3, 19-20.

7. The use of AI tools, including large language models, further complicates the risk profile. If DOGE integrates SSA data into any AI system the data may be retained in the model in ways that cannot later be reversed. Even brief access can result in permanent informational extraction, even if formal access is later revoked.[3]

8. Researchers have uncovered methods for data exposure from AI tools using straightforward prompts. For example, using a portion of the text of a news article to get the system to produce more verbatim text from that news article. If these systems are being given access to personally identifiable information at scale, related adversarial methods could be used by bad actors to potentially exfiltrate information and use it to commit fraud.[4]

9. In my previous declaration, I posed a theoretical example of how Grok, an AI tool owned by Elon Musk, could unfairly benefit if trained on sensitive SSA data. In the subsequent days, public reporting alleged that DOGE has indeed "heavily" deployed Grok as part of their work.[5] To my knowledge, Grok has not been vetted and approved for federal use via the Federal Risk and Authorization Management Program, does not use government servers, and has not completed other means to ensure that this cloud-based tool has been vetted for government use.

10. DOGE's request for expansive and expedited access to SSA systems, which hold information on essentially every living American, presents an unacceptable risk and would meaningfully make Americans less safe.

Executed on April 10, 2025, in Washington, D.C.

Erie Meyer

[3] Apostol Vassilev et al., *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*, U.S. Dep't of Commerce xii, 40 (March 2025), https://perma.cc/9HKR-YAER.
[4] Ellen Su et al., *Extracting Memorized Training Data Via Decomposition*, arXiv 1-2 (Oct. 1, 2024), https://perma.cc/2E53-TD3G.
[5] Alexandra Ulmer et al., *Exclusive: Musk's DOGE using AI to snoop on U.S. federal workers, sources say*, Reuters (April 8, 2025), https://perma.cc/F327-EURP.