DOGE Put Critical Social Security Data at Risk, Whistle-Blower Says

DOGE team members uploaded a database with the personal information of hundreds of millions of Americans to a vulnerable cloud server, according to the agency's chief data officer.

Listen to this article · 10:29 min Learn more

By Nicholas Nehamas
Reporting from Washington

Aug. 26, 2025

Members of the Department of Government Efficiency uploaded a copy of a crucial Social Security database in June to a vulnerable cloud server, putting the personal information of hundreds of millions of Americans at risk of being leaked or hacked, according to a whistle-blower complaint filed by the Social Security Administration's chief data officer.

The database contains records of all Social Security numbers issued by the federal government. It includes individuals' full names, addresses and birth dates, among other details that could be used to steal their identities, making it one of the nation's most sensitive repositories of personal information.

The account by the whistle-blower, Charles Borges, underscores concerns that have led to lawsuits seeking to block young software engineers at the agency built by Elon Musk from having access to confidential government data. In his complaint, Mr. Borges said DOGE members copied the data to an internal agency server that only DOGE could access, forgoing the type of "independent security monitoring" normally required under agency policy for such sensitive data and creating "enormous vulnerabilities."

Mr. Borges did not indicate that the database had been breached or used inappropriately.

But his disclosure stated that as of late June, “no verified audit or oversight mechanisms” existed to monitor what DOGE was using the data for or whether it was being shared outside the agency. That kind of oversight would typically be provided by the agency’s career information security professionals, Mr. Borges said in his account.

And his complaint cites an official agency security assessment that described the project as “high risk” and that warned of “catastrophic impact” to Social Security beneficiaries and programs if the database were to be compromised.

“Should bad actors gain access to this cloud environment, Americans may be susceptible to widespread identity theft, may lose vital health care and food benefits, and the government may be responsible for reissuing every American a new Social Security number at great cost,” Mr. Borges’s complaint said. He alleged that DOGE did not involve him in discussions about the project, despite his role as chief data officer, leaving him to piece together evidence of what had happened after the fact.

Included in his account, a copy of which was reviewed by The New York Times, are more than two dozen pages of internal emails, memos and other records to document his claims. Mr. Borges’s complaint said that DOGE’s actions “potentially violated multiple federal statutes” designed to protect government data.

Lawyers at the Government Accountability Project, a whistle-blower protection group, filed Mr. Borges’s account on Tuesday with the Office of Special Counsel as well as with congressional lawmakers. Mr. Borges, 49, joined the Social Security Administration in January after working for more than three years at other government agencies, including the Centers for Disease Control and Prevention, and serving 22 years in the Navy, according to his complaint. His lawyers declined to make him available for an interview with The Times.

A spokesman for the Social Security Administration, Nick Perrine, said that the agency took whistle-blower complaints seriously.

“S.S.A. stores all personal data in secure environments that have robust safeguards in place to protect vital information,” he said. “The data referenced in the complaint is stored in a longstanding environment used by S.S.A. and walled off from the internet. High-level career S.S.A. officials have administrative access to this system with oversight by S.S.A.’s information security team.”

Mr. Perrine added that the agency was “not aware of any compromise to this environment” and remained “dedicated to protecting sensitive personal data.”

A White House spokeswoman referred questions to the Social Security Administration.

The complaint includes documents showing that DOGE leaders sought to upload the data despite warnings that they could be exposing Americans’ personal information. The documents do not reveal why DOGE pushed for the project, although Mr. Borges said he was later told that the reason was to improve the way the agency exchanged data with other parts of government.

“I have determined the business need is higher than the security risk associated with this implementation and I accept all risks,” wrote Aram Moghaddassi, who worked at two of Mr. Musk’s companies, X and Neuralink, before becoming Social Security’s chief information officer, in a July 15 memo.

Mr. Moghaddassi did not immediately respond to a request for comment.

DOGE’s access to Social Security data became one of the earliest flash points in Mr. Musk’s contentious spell in Washington. The billionaire and his allies pushed for DOGE to have unfettered access to the agency’s data, which is strictly protected under federal law, ousting career officials who stood in their way. Mr. Musk advanced false claims of widespread fraud at Social Security to justify the urgency of DOGE’s work.

Privacy advocates and Democrats warned that the confidentiality of Americans' personal information might be at risk. Social Security data is highly sought after by criminals and foreign governments, who can use the information for identity theft or to gather intelligence. A federal judge temporarily blocked DOGE's access to sensitive Social Security data in March, but the Supreme Court overruled that decision on June 6.

The agency has also shared data with immigration authorities, as President Trump seeks to carry out his mass deportation agenda.

Although Mr. Musk and many of his allies left Washington after the billionaire fell out with Mr. Trump in May, members of DOGE have continued to occupy key roles in the federal bureaucracy, including Mr. Moghaddassi.

At issue in Mr. Borges's complaint is the so-called Numident file, a critical database that contains the personal information of everyone who has ever held a Social Security number, living or dead. The agency has issued more than 548 million numbers.

In his complaint, Mr. Borges provided documents showing that DOGE member John Solly, a software engineer working at Social Security, called a career agency employee on June 10 to open discussions about copying Numident data to a "virtual private cloud" server operated by Social Security. Edward Coristine, a 19-year-old DOGE software engineer, was also involved in the project and would be given access to the server, other records show. The request came shortly after the Supreme Court allowed members of DOGE to have access to the agency's data.

Mr. Solly and Mr. Coristine did not immediately respond to requests for comment.

At least one senior official soon began raising concerns, according to documents disclosed in Mr. Borges's complaint.

On June 16, Joe Cunningham, the agency's acting chief information security officer, emailed Mr. Moghaddassi and another top official, attaching a copy of an official risk assessment.

“After a thorough review, we have determined that this request poses a high risk,” Mr. Cunningham wrote, adding that “our current policy requires sign-off from the chief information officer (C.I.O.) to accept these risks.”

The risk assessment stated that DOGE wanted “uninhibited” control over the server to “expedite” its work but had not provided documentation of how it would maintain security, and it warned that “sensitive data could be made public,” according to a copy included in Mr. Borges’s complaint.

In another email to colleagues on June 23, Mr. Cunningham wrote: “We need to address how we can effectively monitor the data and the security controls that will be implemented.”

Two days later, he asked Michael Russo, a senior DOGE-aligned official at Social Security, to sign off on the project, noting that the personal data being uploaded had not been “sanitized,” or anonymized, as he suggested would typically be the case.

“Approved,” Mr. Russo replied less than half an hour later.

Another Social Security employee wrote that a colleague would be “transferring a copy of the Numident data over shortly.”

Mr. Russo declined to comment. Mr. Cunningham did not immediately respond.

Mr. Borges’s complaint stated that he was kept in the dark about copying the Numident data and that his superiors did not address his concerns when he raised them this month.

And he said that after he started asking questions about the project, the agency’s Office of the General Counsel told employees “not to respond to his inquiries.”

“Mr. Borges spent weeks pressing for fixes inside” the agency, Andrea Meza, a lawyer with the Government Accountability Project, said in a statement. “When nothing changed, he used the protected channels federal whistle-blower law provides.”

Mr. Borges's complaint also includes documents that he said backed up two additional allegations.

He said that in March DOGE officials bypassed normal security procedures and were given "improper and excessive access" to other databases that contained sensitive information about Social Security applicants, including the ability to edit data.

Mr. Borges also said that DOGE officials briefly "appeared to have circumvented" the March 20 temporary court order that locked them out of Social Security data, regaining access to the data over the following weekend before being cut off again on March 24.

Aric Toler contributed reporting. Kirsten Noyes and Emily Powell contributed research.

Nicholas Nehamas is a Washington correspondent for The Times, focusing on the Trump administration and its efforts to transform the federal government.

A version of this article appears in print on , Section A, Page 1 of the New York edition with the headline: DOGE Risked Personal Data, An Insider Says