Social Security Administration Exec Whistleblower Quits After Alleging Security Breach

Chuck Borges sent his resignation email to Social Security Administration staff on a Friday morning, claiming he had been forced out after blowing the whistle on what he called dangerous mishandling of Americans' personal data. But about 30 minutes later the email had mysteriously disappeared from employee inboxes.

He was the chief data officer and had filed a formal complaint just days earlier accusing DOGE of creating an unsecured copy of the nation's entire Social Security database. The database, known as NUMIDENT, contains birth dates, parents' names, addresses and Social Security numbers for more than 300 million Americans.

He Quit Because of Retaliation

"This involuntary resignation is the result of SSA's actions against me, which make my duties impossible to perform legally and ethically," Borges wrote in the letter obtained by WIRED magazine.

The complaint filed with the Office of Special Counsel claims DOGE officials systematically bypass security measures to gain unprecedented access to sensitive government data.

According to the letter (which is attached here), 19-year-old Edward Coristine, known by the nickname "Big Balls," was among those granted access despite a history that included involvement with a cybercrime group.

In March, when a federal court ordered SSA to revoke DOGE's access to the data, agency officials initially complied. But within 24 hours, according to Borges' complaint, senior career officials received instructions to restore access, granting even broader privileges than before.

Your Data Is Now In The Cloud With Very Little Security

The whistleblower complaint describes how John Solly, identified as a DOGE-aligned hire, requested in June that the entire SSA database be copied to a cloud environment. When career officials warned this posed "very high risk" and could have "catastrophic impact to SSA beneficiaries," the transfer was approved anyway.

Michael Russo, who served briefly as SSA's chief information officer despite having no known government experience, gave his approval with a simple "Approved”

The cloud environment lacked basic security controls that are standard for government systems. There was no tracking of who accessed the data or how they used it, no independent oversight and no audit mechanisms, according to Borges.

A Massive Breach In The Making

"If this information were to be compromised, it is possible that the sensitive PII on every American including health diagnoses, income levels and banking information, family relationships, and personal biographic data could be exposed publicly," the complaint states. The government might need to reissue Social Security numbers to every American if the data were breached.

Borges had tried to raise concerns internally before going to outside authorities. In August, he sent emails to various SSA offices requesting information about data security in the cloud environments.

GOVERNMENT ACCOUNTABILITY PROJECT

1612 K Street NW Suite #808
Washington, DC, 20006
(202) 457-0034
whistleblower.org

August 26, 2025

Sent via electronic mail

Honorable Rand Paul, Chair
Honorable Gary Peters, Ranking Member
Senate Committee on Homeland Security & Governmental Affairs
Washington, D.C. 20510

Honorable James Comer, Chair
Honorable Ranking Member, Robert Garcia
House Committee on Oversight and Government Reform
Washington, DC 20515

Honorable Mike Crapo, Chair
Honorable Ron Wyden, Ranking Member
Senate Committee on Finance
Washington, D.C. 20510

Honorable Jason Smith, Chair
Honorable Richard E. Neal, Ranking Member
House Ways and Means Committee
Washington D.C. 20515

Jamieson Greer
Acting Special Counsel
U.S. Office of Special Counsel
1730 M Street, NW, Suite 218
Washington, D.C. 20036

Re: Protected Whistleblower Disclosure of Charles Borges Regarding Violation of Laws, Rules & Regulations, Abuse of Authority, Gross Mismanagement, and Substantial and Specific Threat to Public Health and Safety at the Social Security Administration

Dear All:

The Government Accountability Project represents Mr. Chuck Borges, the Chief Data Officer (CDO) at the Social Security Administration (SSA), and a whistleblower. Mr. Borges presents the following disclosures to your attention pursuant to 5 U.S.C. § 2302, 5 U.S.C. § 1213 and 5 U.S.C § 7211 for your respective offices to take appropriate oversight action.

In recent weeks Mr. Borges has become aware through reports to him of serious data security lapses, evidently orchestrated by DOGE officials, currently employed as SSA employees, that risk the security of over 300 million Americans' Social Security data.[1] Mr. Borges' disclosures involve wrongdoing including apparent systemic data security violations, uninhibited administrative access to highly sensitive production environments,[2] and potential violations of

[1] Social Security Administration. "Social Security performance." https://www.ssa.gov/ssa-performance.
[2] Production systems are operational settings where applications or data serve real users. For example, when a website is created, it is not written and published at the same time; if it were written and published simultaneously, the website could break or a vulnerability could be introduced. Instead, a website is first created in a "development environment" then is published in a production environment. Ideally, production data and the production environment are tightly controlled. In cases where production data might be used for development, it is critical to have rigorous security in place. "Exposing production data to test environments comes with risks, such as potential data breaches and regulatory

internal SSA security protocols and federal privacy laws by DOGE personnel Edward Coristine, Aram Moghaddassi, John Solly, and Michael Russo.[3] These actions constitute violations of laws,

non-compliance." "What is Production data?", *Accelario*, Accessed August 20, 2025. https://accelario.com/glossary/production-data/.

[3] Edward Coristine, nicknamed "Big Balls," is a 19-year-old programmer for DOGE. In February 2025, he was listed as staff at the Cybersecurity and Infrastructure Security Agency, then joined the Department of Government Efficiency as a "Senior Advisor" after interning at one of Elon Musk's companies, Neuralink. He became a full-time government employee in May 2025, where he earned one of the highest salaries possible for federal employees as a GS-15. Makena Kelly, "'Big Balls' Is Officially a Full-Time Government Employee.", *Wired*, June 4, 2025. https://www.wired.com/story/big-balls-young-doge-converted-into-full-time-government-employees/. Coristine resigned from DOGE in June 2025 and reappeared as part of SSA days later. Jake Lahut, Makena Kelly, Vittoria Elliott, and Zoë Schiffer, "'Big Balls' No Longer Works for the US Government." *Wired*, June 24, 2025. https://www.wired.com/story/big-balls-coristine-doge-resigned-us-government/. Coristine has a lengthy history of facilitating, soliciting, or possibly participating in cybercrime. He was formerly part of a cybercrime group called The Com, responsible for multiple privacy breaches and fraud. A Telegram handle associated with Coristine also hired a hacker in 2022 to complete a DDoS cyberattack. Krebs, Brian. *Teen on Musk's DOGE Team Graduated from 'The Com' – Krebs on Security*. February 28, 2025. https://krebsonsecurity.com/2025/02/teen-on-musks-doge-team-graduated-from-the-com/. He was previously fired from cybersecurity firm Path Networks—a firm which itself hires convicted hackers—for allegedly leaking secrets to a competitor. Jason Leopold, Margi Murphy, Sophie Alexander, Jake Bleiberg, and Anthony Cormier. "Musk's DOGE Teen Was Fired By Cybersecurity Firm for Leaking Company Secrets." *Bloomberg*, February 7, 2025. https://www.bloomberg.com/news/articles/2025-02-07/musk-s-doge-teen-was-fired-by-cybersecurity-firm-for-leaking-company-secrets. Further, one of Coristine's companies, Tesla.Sexy, owns Russian-registered domains targeting the Russian market. Greenberg, Andy. "DOGE Teen Owns 'Tesla.Sexy LLC' and Worked at Startup That Has Hired Convicted Hackers." *Wired*, February 6, 2025. https://www.wired.com/story/edward-coristine-tesla-sexy-path-networks-doge/.

Like Coristine, Moghaddassi has previously worked for Musk's companies, Neuralink and X. Moghaddassi formerly worked for DOGE at the Department of Labor. He has been a software engineer for DOGE at the SSA since March, and in June 2025, Moghaddassi became the CIO for the SSA. Gickling, Steve. "SSA Appoints Aram Moghaddassi as CIO." *DevX*, July 8, 2025. https://www.devx.com/daily-news/ssa-appoints-aram-moghaddassi-as-cio/. Coristine and Moghaddassi have previously been given access to vast amounts of sensitive immigration data and IT systems at United States Citizenship and Immigration Services. They were also granted access to USCIS' cloud-based "data lake" and other enabling technologies like Github. Rebecca Heilweil, "DOGE Granted Access to Naturalization-Related IT Systems, Memo Shows." *FedScoop*, April 2, 2025. https://fedscoop.com/doge-granted-access-to-naturalization-immigration-it-systems/. In April 2025, Moghaddassi sent acting SSA Commissioner Leland Dudek a list of 6,300 immigrants whose parole status was revoked the same day. Although Moghaddassi claimed the list included only people on the "terrorist watch list" or having "FBI criminal records," his list included eight minors, including one 13-year-old, calling into question the list's veracity. Alexandra Berzon, Hamed Aleaziz, Nicholas Nehamas, Ryan Mac, and Tara Siegel Bernard. "Social Security Lists Thousands of Migrants as Dead to Prompt Them to 'Self-Deport.'" *New York Times*, April 10, 2025. https://www.nytimes.com/2025/04/10/us/politics/migrants-deport-social-security-doge.html. Moghaddassi claimed on Fox News in March that "40% of the phone calls [Social Security] gets are from fraudsters," statements that likely contributed to the elimination of SSA's phone services in April. *Elon & DOGE Team Sit down with Bret Baier*. Special Report with Bret Baier. Fox News Channel, 2025. https://www.facebook.com/watch/?v=916344540452947, 10:15.

John Solly, described as a DOGE-aligned hire, reportedly joined the SSA in March 2025 in the office of the CIO. Makena Kelly, "This Is DOGE 2.0." *Wired*, July 10, 2025. https://www.wired.com/story/next-stage-doge-elon-musk/.

Michael Russo served as Chief Information Officer of the SSA from February 2025 until late March 2025, when he was replaced by Scott Coulter and transitioned to a special advisor role in SSA focused on "modernizing its archaic technology." Natalie Alms, "Scott Coulter will replace the agency's previous CIO, who has been moved to a senior advisor position at SSA." *NextGov*, March 25, 2025. https://www.nextgov.com/people/2025/03/ssa-tech-shop-be-led-another-doge-associate/404031/. Russo, called "DOGE-aligned" by Wired, was appointed on January 30, 2025, by President Trump despite possessing no known government experience (previously serving as an executive at Shift4, a payment processing company) and requested access, in the face of resistance from senior SSA officials at

rules, and regulations, abuse of authority, gross mismanagement, and creation of a substantial and specific threat to public health and safety.

Since February 2025, it has been widely reported that DOGE officials have sought to access the American public's Social Security data, purportedly to address claims of fraud.[4] A lawsuit has been filed, resulting in a temporary restraining order, to limit DOGE's access to this sensitive data.[5] What has not been reported are DOGE's actions, in violation of SSA protocols and policies, under the authority of SSA Chief Information Officer (CIO) Aram Mogaddassi, to create a live copy of the country's Social Security information in a cloud environment that circumvents oversight.

This vulnerable cloud environment is effectively a live copy of the entire country's Social Security information from the Numerical Identification System (NUMIDENT) database, that apparently lacks any security oversight from SSA or tracking to determine who is accessing or has accessed the copy of this data. NUMIDENT contains all data submitted in an application for a United States Social Security card—including the name of the applicant, place and date of birth, citizenship, race and ethnicity, parents' names and social security numbers, phone number, address, and other personal information. Should bad actors gain access to this cloud environment, Americans may be susceptible to widespread identity theft, may lose vital healthcare and food benefits, and the government may be responsible for re-issuing every American a new Social Security Number at great cost.

Mr. Borges' reports, supported by documentary evidence, reveal a disturbing pattern of questionable and risky security access and administrative misconduct that implicates some of the public's most sensitive data. Mr. Borges has raised concerns internally with various authorities in the Chief Information Officer's (CIO) office and to date has not been made aware of any remedial action. He therefore elevates his concerns out of a sense of urgency and duty to the American public.

Since February, several members of Congress have written letters and opened

---

the time, to SSA data to investigate claims of fraud from Elon Musk and Trump. Makena Kelly, David Gilbert, "These Are the 10 DOGE Operatives Inside the Social Security Administration." *Wired*, March 13, 2025. https://www.wired.com/story/doge-operatives-access-social-security-administration/. Reporting from the New York Times suggests Russo disregarded an investigation by SSA public servants into Musk and Trump's claims of fraud, and instead directed Akash Bobba – a 21-year-old former Palantir intern – to conduct his own analysis of these claims using SSA's personal data of Americans. Alexandra Berzon, Nicholas Nehamas, and Tara Siegel Bernard, "The Bureaucrat and the Billionaire: Inside DOGE's Chaotic Takeover of Social Security." *New York Times*, June 16, 2025. https://www.nytimes.com/2025/06/16/us/politics/doge-social-security.html.

[4] PBS News, "Social Security Head Steps down over DOGE Access of Recipient Information, AP Reports." February 18, 2025. https://www.pbs.org/newshour/politics/social-security-head-steps-down-over-doge-access-of-recipient-information-ap-reports.

[5] American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland, February 21, 2025), ECF No. 1, https://www.courtlistener.com/docket/69664313/1/american-federation-of-state-county-and-municipal-employees-afl-cio-v/.

investigations to demand greater oversight over DOGE's access to SSA data.[6] We urge all members of Congress committed to the safety of their constituents' data along with the U.S. Office of Special Counsel to investigate the disclosures presented in this letter.

I. Background on SSA CDO Charles Borges

Mr. Charles Borges, serving as the CDO of the SSA since January 27, 2025, is a career civil servant and a decorated veteran having served 22 years in the U.S. Navy, including a deployment during 9/11, and was awarded the Air Medal with the Combat Distinguishing Device for individual action in Operation Iraqi Freedom. Mr. Borges has spent the last approximately 10 years — first as an Active Duty Naval Officer then as a civil servant — working for federal public agencies on IT, data architecture, security, and analytics initiatives and throughout his career has developed extensive expertise in data management and business analytics.[7]

Before joining SSA, Mr. Borges held several civil service positions, including at the General Services Administration (GSA), the Office of Management and Budget (OMB), and the Centers for Disease Control and Prevention (CDC) during COVID-19. At the CDC, he contributed to data strategy by developing methods and metrics for measuring advances in public health, and played a key role in the Public Health Data Modernization Initiative.[8] He has also served as a White House Presidential Innovation Fellow, supporting key federal data initiatives like providing feedback on executive orders and contributing to the Federal Data Strategy, the 10 year vision for the federal government's use of data.[9]

---

[6] "Larson and Ways and Means Committee Democrats Demand Answers from Social Security Administration on Dodgy 'DOGE' Access to Payment Systems | Congressman John Larson." February 11, 2025. http://larson.house.gov/media-center/press-releases/larson-and-ways-and-means-committee-democrats-demand-answers-social; "Norton, House Oversight Committee Members, and Warren Open Investigation Into DOGE.Gov After Alarming Failures to Protect Sensitive National Security Information | Congresswoman Eleanor Holmes Norton." February 28, 2025. http://norton.house.gov/media/press-releases/norton-house-oversight-committee-members-and-warren-open-investigation-dogegov; "Warren, Wyden, Sanders, Gillibrand Demand Answers on 'Reckless' AI Tool Rollout at SSA | U.S. Senator Elizabeth Warren of Massachusetts." Accessed August 18, 2025. https://www.warren.senate.gov/newsroom/press-releases/warren-wyden-sanders-gillibrand-demand-answers-on-reckless-ai-tool-rollout-at-ssa; "Peters Presses Agency Leaders on DOGE Access to Federal IT Systems and Data Repositories | U.S. Senator Gary Peters of Michigan." March 27, 2025. https://www.peters.senate.gov/newsroom/press-releases/peters-presses-agency-leaders-on-doge-access-to-federal-it-systems-and-data-repositories.

[7] Mr. Borges holds a Bachelor of Science in Astronomy from the Massachusetts Institute of Technology, a Master of Science in Aviation Systems from the University of Tennessee, and an MBA from the University of Maryland, and certifications as a Certified Scrum Product Owner, an AWS Certified Cloud Practitioner, and a Certified Data Management Professional.

[8] The CDC's Public Health Data Modernization Initiative is a large scale and far-reaching data project to strengthen and unify critical public health data across the country. It is focused on improving public health data to make it more accessible, flexible, equitable, and usable for action. US Centers for Disease Control and Prevention. "Data Modernization Initiative (DMI)." https://www.cdc.gov/data-modernization/php/about/dmi.html.

[9] CDO Magazine. "Social Security Administration Appoints Chuck Borges as Chief Data Officer." Accessed August 15, 2025. https://www.cdomagazine.tech/leadership-moves/social-security-administration-appoints-chuck-borges-as-chief-data-officer; "Federal Data Strategy —Data, accountability, and transparency: creating a data strategy and

During his twenty-two years of Navy service, Mr. Borges specialized in data analytics, standing up a new data team to analyze and address the physiological impacts of low oxygen on pilots in T-45 aircraft who went on extended safety stand down because of the effects of low oxygen levels in the aircraft. He previously served as Chief Data Officer for Naval Air Systems Command (NAVAIR) and Military Director of Analytics for the Naval Air Warfare Center Aircraft Division.[10]

On January 27, 2025, Mr. Borges began his role as CDO of SSA leading the Office of Analytics, Review, and Oversight. In this role, Mr. Borges is responsible for the safety, integrity, and security of the public's data at SSA, which includes ensuring compliance with federal data privacy, security, and regulatory requirements as well as internal policies and industry best practices. His position requires full visibility into data access, data exchange, and cloud-based environments used for SSA production systems.

II. Safety Requirements for SSA Data

SSA's administrative role is broad and impacts hundreds of millions of Americans across several functions. For instance, SSA's total benefits disbursements amount to more than 1.5 trillion dollars annually with more than one in five Americans receiving benefits from the agency.[11] SSA has also issued more than 450 million Social Security Numbers to U.S. Citizens and eligible noncitizens,[12] supports the administration of federal programs like Medicare, Medicaid, SNAP, eVerify,[13] assists with voter verification,[14] and collects tax and earnings information.[15] In order to execute these functions, SSA collects and stores personally identifiable information about millions of Americans.[16]

If this information were to be compromised, it is possible that the sensitive PII on every American including health diagnoses, income levels and banking information, family relationships, and personal biographic data could be exposed publicly, and shared widely. Bad actors could use this information to engage in identity theft and to target people based on their

---

infrastructure for the future", *Federal Data Strategy*, Accessed August 20, 2025. https://strategy.data.gov/

[10] CDO Magazine, "Social Security Administration Appoints."

[11] "Fact Sheet." Uploaded March 15, 2025, Social Security Administration, https://perma.cc/595S-B36F.

[12] Carolyn Puckett, "The Story of the Social Security Number." *Social Security Bulletin* 69, no. 2 (2009). https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

[13] "What Is E-Verify | E-Verify." August 19, 2025. https://www.e-verify.gov/about-e-verify/what-is-e-verify.

[14] "Help America Vote Verification (HAVV) Transactions by State." Social Security Administration. https://www.ssa.gov/data/havv/.

[15] Anya Olsen, and Russell Hudson, "Social Security Administration's Master Earnings File: Background Information." *Social Security Bulletin* 69, no. 3 (2009). https://www.ssa.gov/policy/docs/ssb/v69n3/v69n3p29.html#:~:text=SSA%20uses%20this%20information%20to,subject%20to%20IRS%20disclosure%20rules.

[16] "'Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." SSA, citing Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, Managing Information as a Strategic Resource (2016), https://perma.cc/L3CV-M6RF.

unique vulnerabilities. Critical benefits for seniors who have long paid into the Social Security system could be at risk, particularly if the SSA needed to re-issue Social Security Numbers to all Americans in the event of a data breach. Reporting suggests that DOGE could be seeking this data to train and enhance AI models.[17]

Recognizing the importance of safeguarding the public's data, Congress has enacted comprehensive privacy and information security protections for government information systems. Information systems at SSA are subject to even more stringent privacy protections given the breadth and sensitivity of the confidential information they contain. As a memorandum opinion by District Judge Ellen Lipton Hollander for *AFL-CIO v. SSA* notes, "the SSA is subject to a "panoply of laws" that govern and protect SSA's data systems and the disclosure of information held by SSA. These include the Privacy Act, the Social Security Act, the Tax Reform Act of 1976, the Taxpayer Browsing Protection Act, and the Federal Information Security Modernization Act (FISMA)."[18] Other protective statutes of relevance include the Computer Fraud and Abuse Act, the Fair Credit Reporting Act, and the Inspector General Act.

III. DOGE Access to SSA Data

After its founding on January 20, 2025, DOGE employees promptly began requesting internal data from the SSA in February.[19] Former SSA Chief of Staff Tiffany Flick testified that DOGE's rationale for investigating the SSA was "based on an inaccurate understanding of SSA's data and programs"[20]—the data request was partially prompted by unsubstantiated claims by DOGE founder Elon Musk's comments that social security was "the biggest Ponzi scheme of all time."[21]

Under the auspices of its investigation, DOGE personnel have tried to access sensitive

---

[17] Molly Weston Williamson, "DOGE's Data Digging at the Social Security Administration Puts Millions of Americans at Risk." *Center for American Progress*, April 28, 2025. https://www.americanprogress.org/article/doges-data-digging-at-the-social-security-administration-puts-millions-of-americans-at-risk/.

[18] American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland Mar 20, 2025) ECF No. 49, Memorandum Opinion at pp. 17-18 (citing case filings), https://www.courtlistener.com/docket/69664313/49/american-federation-of-state-county-and-municipal-employees-afl-cio-v/.

[19] Leah Feiger, "Elon Musk's DOGE Is Getting Audited." *Wired*, April 9, 2025. https://www.wired.com/story/gao-audit-elon-musk-doge-government-agencies/. PBS News. "Social Security Head Steps down over DOGE Access of Recipient Information, AP Reports." February 18, 2025. https://www.pbs.org/newshour/politics/social-security-head-steps-down-over-doge-access-of-recipient-information-ap-reports.

[20] Martin Pengelly, "Doge Takeover of Social Security Seemed 'Based on Myth', Says Ex-Senior Official." US News. *The Guardian*, March 10, 2025. https://www.theguardian.com/us-news/2025/mar/10/elon-musk-doge-social-security; American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland Mar 07, 2025) ECF No. 22, Exhibit J at p. 6, https://www.courtlistener.com/docket/69664313/22/10/american-federation-of-state-county-and-municipal-employees-afl-cio-v/

[21] *Joe Rogan Experience #2281 - Elon Musk*. 2025. https://www.youtube.com/watch?v=sSOxPJD-VNo&t=6703s, 1:01:58.

SSA data.[22] Indeed, former SSA Acting Commissioner Michelle King resigned in February after refusing to hand over unprecedented amounts of sensitive, protected information—possibly including addresses, banking information, medical records, income information, and employment history—to DOGE.[23] Despite such strong opposition, some sources report that DOGE has had read-access to SSA data since at least March, allowing employees to potentially copy data for unauthorized purposes.[24]

Several federal auditors have denounced DOGE's work as improper, in violation of established standards on assessing government work, and possibly an excuse to "steal a vast amount of government data."[25] Concerns have also arisen about the questionably high information clearances provided on short notice to employees lacking government experience. For example, SSA-assigned DOGE employee Edward Coristine became a federal employee at 19-years-old yet received high security clearances and extensive access to sensitive information.[26] Concerned lawmakers and government agencies have attempted to use audits and

---

[22] Further, in their "audit" of the SSA, the DOGE team followed their pattern of accessing multiple agencies' data systems without proper understanding of its context, leading to erroneous conclusions (such as claims that deceased individuals or 150-year-olds were receiving social security), error-riddled published findings, and even dangerous information practices. David Gilbert, "No, 150-Year-Olds Aren't Collecting Social Security Benefits." *Wired*, February 17, 2025. https://www.wired.com/story/elon-musk-doge-social-security-150-year-old-benefits/; Fowler, Stephen. "DOGE's Savings Page Fixed Old Mistakes — and Added New Ones." Politics, *NPR*, March 1, 2025. https://www.npr.org/2025/03/01/nx-s1-5313853/doge-savings-receipts-musk-trump. In April 2025, a whistleblower exposed DOGE's unsafe and potentially unlawful plan to create a "master database" of confidential SSA information, increasing the risk and impact of devastating data breaches. Gerald Connolly, April 17, 2025. https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025-04-17.gec-to-ssa-oig-master-data.pdf at p. 5; "Disturbing Whistleblower Information Obtained by Committee Democrats Leads Ranking Member Connolly to Demand Investigation into DOGE's Disruption of Social Security Operations, Collection of Americans' Sensitive Data | The Committee on Oversight and Accountability Democrats." April 17, 2025. http://oversightdemocrats.house.gov/news/press-releases/disturbing-whistleblower-information-obtained-committee-democrats-leads-ranking.
DOGE employee Steve Davis reportedly told SSA officials that DOGE would link data sources with the ultimate goal of "joining all data across government," rendering sensitive information extremely vulnerable to hacking. Hannah Natanson, Joseph Menn, Lisa Rein, and Rachel Siegel. *The Washington Post*, May 7, 2025. https://www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security/.
DOGE personnel also allegedly lacked the training to handle sensitive SSA data properly, amplifying the risk of such collected sensitive information falling into the wrong hands. Pengelly, Martin. "Doge Takeover of Social Security."

[23] Neal Broverman, "Addresses, Earnings, Medical Records of Americans Could Be in DOGE's Hands Soon." *Mashable*, February 18, 2025. https://mashable.com/article/doge-social-security-data-risk.

[24] Ash Center. "Understanding DOGE and Your Data." March 31, 2025. https://ash.harvard.edu/resources/understanding-doge-and-your-data/.

[25] Vittoria Elliott, "'It's a Heist': Real Federal Auditors Are Horrified by DOGE." *Wired*, March 18, 2025. https://www.wired.com/story/federal-auditors-doge-elon-musk/.

[26] Vittoria Elliott, "How Edward 'Big Balls' Coristine and DOGE Got Access to a Federal Payroll System That Serves the FBI." *Wired*, July 30, 2025. https://www.wired.com/story/edward-coristine-big-balls-doge-federal-pay-roll-system/; Congress of the United States (James A. Hines, Ranking Member House Permanent Select Committee on Intelligence et al.) to The Honorable Donald J. Trump, President of the United States, February 4, 2025, https://democrats-intelligence.house.gov/uploadedfiles/rm_letter_to_potus_signed.pdf (seeking answers regarding the granting of security clearances to DOGE affiliates and their access to sensitive government data and information systems).

legal actions to thwart DOGE's invasive SSA data access, to little avail.[27]

IV. Lawsuit Results in Temporary Restraining Order Preventing DOGE Access

On February 21, 2025, plaintiffs American Federation of State, County & Municipal Employees AFL-CIO (AFSCME), Alliance for Retired Americans (ARA), and American Federation of Teachers (AFT) sued SSA, Acting Commissioner of SSA Leland Dudek, and DOGE seeking to halt the access by DOGE personnel without proper security clearance of SSA's PII on the American Public.[28]

Between March 20, 2025 and June 6, 2025, the SSA was the subject of a Temporary Restraining Order (TRO) and later a Preliminary Injunction (PI) enjoining and restraining certain entities within the SSA from accessing, using, or disclosing any personally identifiable information related to SSA systems.[29] The TRO enjoined and restrained the Defendants from accessing, using, or disclosing any personally identifiable information related to SSA systems, specifically:

- prohibiting SSA from granting DOGE and its affiliates access to PII "obtained, derived, copied, or exposed from any SSA system of record" including the "Enterprise Data Warehouse (EDW), Numident, Master Beneficiary Record (MBR), and Supplemental Security Record (SSR)";

- ordering DOGE and its affiliates to delete all "non-anonymized PII [SSA] data"

---

[27] In April, Representative Gerald Connolly demanded an investigation into DOGE's data handling by the SSA OIG's Acting Inspector General. "Disturbing Whistleblower Information Obtained." The Government Accountability Office began auditing DOGE's data handling practices at the SSA potentially as early as March, yet reported collaborating with DOGE in April. Leah Feiger, "Elon Musk's DOGE."; Matt Bracken, "After a Slow Start, GAO Says It's Now Hearing from DOGE." *FedScoop*, April 10, 2025. https://fedscoop.com/gao-audit-doge-government-efficiency-work/. In June, senators proposed the Protecting Seniors' Data Act of 2025, requesting a "comprehensive audit" of DOGE's work at the SSA, but the bill has not advanced since its introduction in early June. Matt Bracken, "Senate Democrats Seek Audit of DOGE Access to Social Security Systems." *FedScoop*, June 5, 2025. https://fedscoop.com/senate-democrats-seek-audit-of-doge-access-to-social-security-systems/; "S.1943 - Protecting Seniors' Data Act of 2025." https://www.congress.gov/bill/119th-congress/senate-bill/1943/cosponsors?s=1&r=75.

[28] American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland, February 21, 2025), ECF No. 1, Complaint at p.4, https://www.courtlistener.com/docket/69664313/1/american-federation-of-state-county-and-municipal-employees-afl-cio-v/. On March 7, 2025, the Plaintiffs added as Defendants the Chief Information Officer of the Social Security Administration, the DOGE Acting Administrator, and Elon Musk as Senior Advisor to the President and de facto head of DOGE. American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland, March 07, 2025) ECF No. 17, Amended Complaint against All Defendants Redline Against Original Complaint at pp. 1-2, https://www.courtlistener.com/docket/69664313/17/1/american-federation-of-state-county-and-municipal-employees-afl-cio-v/.

[29] American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland, April 17, 2025) ECF No. 147, Order on Motion for Preliminary Injunction, https://www.courtlistener.com/docket/69664313/147/american-federation-of-state-county-and-municipal-employees-afl-cio-v/.

placed in their possession since January 20, 2025.[30]

Following this order, on March 24, 2025, the SSA Defendants certified compliance with the TRO to the Court. They claimed under oath that:

- SSA has revoked all SSA DOGE Team members' access to SSA systems of records, including but not limited to the Enterprise Data Warehouse, Numident, Master Beneficiary Record, and Supplemental Security Record.

- Any software installed since January 20, 2025, by SSA DOGE Team members or DOGE Affiliates on SSA devices, information systems, or systems of records, or installed on their behalf or on behalf of the DOGE Defendants, has been removed.

- No DOGE personnel would be provided with access to any SSA system without completing standard training;

- No DOGE personnel would be provided with access to any SSA system without a background check;

- No DOGE detailee to SSA would have access to any SSA system without a completed detail agreement;

- SSA did not seek to provide SSA DOGE team members with Team Members with access to "discrete, particularized, and non-anonymized data" as permitted under the conditions contained in paragraph 3 of the Order.[31]

On March 27, 2025, the Court extended the TRO through April 17, 2025. On April 17, 2025, the District Court granted a Preliminary Injunction based on the same terms as the TRO.[32] That PI was in place and effective until June 6, 2025, when the Supreme Court stayed the preliminary injunction, allowing DOGE members to access SSA records pending the appeal on the merits in the lower courts.[33]

---

[30] American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland, March 20, 2025) ECF No. 48, Temporary Restraining Order at p. 1, https://www.courtlistener.com/docket/69664313/48/american-federation-of-state-county-and-municipal-employees-afl-cio-v/.

[31] American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland, March 24, 2025) ECF No. 56, Affidavit at pp. 2-3, https://www.courtlistener.com/docket/69664313/56/1/american-federation-of-state-county-and-municipal-employees-afl-cio-v/.

[32] American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, 1:25-cv-00596, (D. Maryland, April 17, 2025) ECF No. 147, https://www.courtlistener.com/docket/69664313/147/american-federation-of-state-county-and-municipal-employees-afl-cio-v/.

[33] Social Security Administration, et al. v. American Federation of State, County, and Municipal Employees, et al.

V. Mr. Borges' Disclosures

a. Hasty, Unjustified Expedited Access to Enterprise Data Warehouse Databases

Beginning around March 14, 2025, DOGE officials were given improper and excessive access to multiple schemas and databases inside the Enterprise Data Warehouse (EDW),[34] including databases and schemas containing sensitive information on SSN Applicants and the application process.

First, around March 14, 2025, DOGE members requested access to PSNAP and SNAP MI databases for Payton Rehling and Aram Moghaddassi. Information reported to Mr. Borges indicates that proper approval through the Systems Access Management (SAM) system was bypassed for this request, which resulted in four user profiles.[35] The Security Access Management process requires a written request for data access that is then either approved or disapproved by a supervisor who provides a written justification for their decision. This process is necessary for oversight of database access approvals.

Additionally, these profiles concerningly included equipment pin access and write access.[36] Equipment pin access means that instead of a user accessing data through a personal pin identifier, which would make the accessor's actions traceable to a user, an equipment pin is used to verify the identity of a device or piece of equipment before it is granted access to a network or sensitive resources, potentially avoiding the creation of a record tied to a specific user. Giving a user "write access" means that the user will have the ability to edit data.

Granting access to databases that exceed authorized permissions violates the principle of least privilege, which holds that users should have the least amount of access necessary to do their job.[37] Information provided to Mr. Borges indicates that on Monday March 17, 2025, the EDW team discovered that users had been given access to data that was reportedly not authorized through normal approval channels.[38]

The improper access to various EDW databases and schemas potentially violated 26 U.S.C. § 6103 (Internal Revenue Code provisions governing Federal Tax Information) as EDW data may contain tax-related information subject to IRS Publication 1075 requirements. The

---

605 U.S. (2025) (June 6, 2025), https://www.supremecourt.gov/opinions/24pdf/24a1063_6j37.pdf.

[34] An Enterprise Data Warehouse (EDW) is a central, secure system that integrates data from various sources across an organization to support informed decision-making and strategic analysis. It acts as a single source of truth, providing a consistent and reliable view of data for reporting, analytics, and business intelligence.

[35] Exhibit 1, p. 5

[36] Exhibit 1, p. 5

[37] Amazon Web Services. "Security best practices in IAM." https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege.

[38] Exhibit 1, p. 5

unauthorized write access also potentially violated 18 U.S.C. § 1030(a)(2) by exceeding authorized access to obtain information from protected computers.

b. DOGE Access Restored in Violation of Court Order and Multiple Federal Statutes

On Thursday, March 20, 2025, the Social Security Administration received the TRO prohibiting DOGE and its affiliates from access to SSA's data and revoked VPN access accordingly.[39] The following day, on Friday, March 21, 2025, the EDW team initially complied with proper procedures by revoking data access through the established SAM request process.[40]

However, within 24 hours of the court-ordered revocation, DOGE officials appeared to have circumvented the judicial mandate. On the evening of Friday, March 21, 2025, according to information later received by Mr. Borges, senior career EDW officials who have system administrative privileges received instructions to undo the court-ordered access restrictions for two DOGE employees.[41]

Furthermore, the requested access was for new and expanded privileges beyond the privileges that were in place at the time of the TRO, totaling forty-two different profiles, including specifically identified privileges that should not have been granted.[42] The information available to Mr. Borges indicates that all access requests were granted.[43]

Then, on March 24, 2025, the Office of Information Security (OIS) revoked DOGE team members' access for profiles that lacked required SAM requests.[44]

This emergency restoration of access raises concerns that the TRO may have been violated and may have also violated federal statutes, potentially including: 18 U.S.C. § 1030 (Computer Fraud and Abuse Act) by facilitating unauthorized access to protected computer systems; 5 U.S.C. § 552a (Privacy Act of 1974) by providing unauthorized access to systems of records containing personally identifiable information without proper justification or approval; 44 U.S.C. § 3551 et seq. (Federal Information Security Modernization Act) by circumventing established security controls and procedures designed to protect federal information systems; 5 U.S.C. Appendix (Inspector General Act) as proper oversight procedures were systematically bypassed, potentially impeding the Inspector General's ability to conduct effective audits and investigations of the agency's operations; and potentially constituted 18 U.S.C. § 371

[39] "Following the court order on Thursday 03/20 - SSA revoked VPN access to SGE team members.", Exhibit 1, p. 6.
[40] "Friday 03/21 - EDW revoked data access - Did we follow SAM here?? TD: Yes, requestors submitted > requestor supervisor> Pam Styles process. These were remove profile requests with all SGEs.", Exhibit 1, p. 6.
[41] Exhibit 1, p. 6
[42] Exhibit 1, p. 6
[43] Exhibit 1, p. 6
[44] Exhibit 1, p. 6

(Conspiracy) to circumvent a federal court order.

c. DOGE Creates Unmonitored Copy of All of SSA's Data on the American Public

In June 2025, following the Supreme Court's stay of the Preliminary Injunction on June 6, 2025,[45] DOGE's access to SSA data escalated in scope and gravity when DOGE personnel appeared to have given themselves authorization to create a copy of SSA's entire set of data on the American public without any independent security or oversight mechanisms in place in violation of laws and creating enormous vulnerabilities.

i. Initial DOGE request

On June 10, 2025, John Solley asked SSA CIO professionals to create a cloud environment[46] to which SSA's Numerical Identification System or "NUMIDENT" data could be transferred.[47] The purported reason for the project was to improve the way that SSA exchanges data. To Mr. Borges' knowledge, such a project is not inherently dangerous, as long as proper security controls are in place.

On June 11, 2025, the request appeared to have changed to a request to transfer NUMIDENT to a test environment.[48] Based on Mr. Borges' experience and expertise, this was an odd but not unheard of request, as it is atypical and strongly discouraged to move production data to a test environment. Later that morning, it became clear that DOGE's request again changed, at this point, they wanted full administrative access to the cloud environment.[49]

ii. OCIO Identifies DOGE Request as Very High Risk

To Mr. Borges' knowledge, on June 12, 2025, a career official in the Office of the Chief Information Officer (OCIO) shared a formal "Risk Acceptance Request Form" with Aram Moghaddassi and an SSA career executive apparently responding to the June 10-11 request to have administrative access to "their own Virtual Private Cloud (VPC, "cloud") within the SSA Amazon Web Services – Agency Cloud Infrastructure (AWS-ACI)."[50] In sharing this risk assessment, the CIO career official noted that the request was "high-risk"[51] due to the proposal to include a replica copy of NUMIDENT, production data considered a High-Value Aset (HVA), in a development environment as "most security exposures and breaches occur within

[45] Social Security Administration, et al. v. American Federation of State, County, and Municipal Employees, et al. 605 U.S. (2025) (June 6, 2025), https://www.supremecourt.gov/opinions/24pdf/24a1063_6j37.pdf.
[46] Mr. Borges does not have knowledge whether this was a development or production environment.
[47] Exhibit 4, p. 25
[48] Exhibit 4, p. 24
[49] Exhibit 4, p. 24
[50] Exhibit 3, p. 12
[51] The risk assessment describes the risk as both "high" and "very high" risk. However, the "Estimated Risk Score" of 15 clearly falls under the "very high" level of impact.

development environments due to reduced control measures and oversight."[52]

NUMIDENT is the Social Security Administration's computer database file containing ***all information submitted in an application for a United States Social Security card*** (Form SS-5), including the name of the applicant, place and date of birth, citizenship, race and ethnicity, parents' names and social security numbers, phone number, address, and other personal information.[53]

Given the sensitivity of the NUMIDENT data, the risk assessment specifically noted four problems with bypassing agency policy, which requires the Division of Infrastructure Services (DIS) to be administrators on the cloud, and instead giving this administrative access to DOGE:

1. The requested VPC project does not have an "Authority to Operate (ATO)"[54] to ensure proper security controls are in place;

2. Developers (presumably DOGE) planned to import NUMIDENT into the cloud, and because AWS-ACI is an extension of the SSA network, any other SSA production data and PII could also be imported; "unauthorized access to the NUMIDENT would be considered ***catastrophic impact to SSA beneficiaries*** and SSA programs" (emphasis added);

3. Because (DOGE) developers, and not DIS, would have administrative access to this cloud, developers would be able to create publicly accessible services, meaning that they would have the ability to allow public access to the system and therefore the data in the system; and

4. Granting (DOGE) developers administrative access would allow them to initiate any AWS service though agency policy required that only DIS could manage such services, meaning that the developers could install services in the cloud not approved for government use.[55]

In order to mitigate the risks of such an "uninhibited development environment," the risk assessment recommended that the cloud project 1) not use production data, 2) work with DIS to ensure agency security policy is followed, and 3) obtain an ATO to ensure proper documentation of controls and risks, per FISMA.[56]

---

[52] Exhibit 3, p. 11
[53] "Application for a Social Security Card." Social Security Administration, https://www.ssa.gov/forms/ss-5.pdf.
[54] An Authority to Operate (ATO) is a formal authorization granted to a system, allowing it to operate on a specific network, typically within a government or regulated environment. It signifies that the system has met required security standards and is deemed acceptable for use. Essentially, an ATO is a "permission slip" for a system to go live and handle sensitive data.
[55] Exhibit 3, p. 13
[56] Exhibit 3, p. 13

The CIO career official submitting the risk assessment to Moghaddassi and the SSA career official noted that "given the high-risk nature of this request," policy required that the Chief Information Officer, Moghaddassi, sign off and approve the risk.[57]

iii. DOGE Given Administrative Access to Cloud Environment, But NUMIDENT Cannot be Transferred Until Security Controls Confirmed

On June 16, 2025, OCIO career staff noted that there were two issues in the risk assessment that should each require their own approval. First, whether DOGE could have administrative access to the requested cloud environment, and second, whether NUMIDENT production data should be moved to this cloud environment.[58]

On June 23, 2025, CIO officials approved DOGE's administrative access to the requested cloud environment, but noted that before being able to approve the request to transfer NUMIDENT data to the cloud, there would need to be "technical discussions" about how to "effectively monitor the data and the security controls," and that the request could not be authorized "until we have a clear understanding of these items."[59] On June 24, 2025, CIO professionals confirmed that DOGE was given administrative access to the cloud.[60]

iv. DOGE-affiliated Michael Russo Approves Transfer of Live NUMIDENT Data to a Cloud Environment Controlled by DOGE and Lacking Independent Security Controls

Mr. Borges has received reports that at some point after DOGE's administrative access was granted on June 24th, a decision was made by OIS that it was impermissible to move NUMIDENT production data to a test cloud environment.

On June 25, 2025, CIO officials elevated a further developed request to Michael Russo.[61] At this point, it appeared that John Solly was requesting that NUMIDENT production data be copied from an environment managed by DIS, per policy, to the DOGE specific cloud environment that lacked independent security controls, and that this requested access bypassed proper SAM protocol.[62] CIO officials, evidently aware of the risk involved in copying "live data rather than the usual sanitized data" typically used for development testing, asked DOGE-affiliated Michael Russo to authorize the transfer of NUMIDENT data.[63] Russo responded to this request with a

[57] Exhibit 3, p. 11
[58] Exhibit 4, pp. 21-22
[59] Exhibit 4, p. 19
[60] Exhibit 4, p. 19
[61] Exhibit 2, pp. 8-9
[62] Exhibit 2, pp. 8-9
[63] Exhibit 2, p. 9

simple, "Approved…."[64]

Mr. Borges reasonably believes that this approval constitutes gross mismanagement, abuse of authority, violation of law, and substantial and specific threat to public health and safety. The transfer of NUMIDENT data to a production account constructed as outlined in the risk assessment above entails replicating live SSA data on millions of Americans to an environment apparently lacking in independent security controls, including independent tracking of who is accessing the data and how they are using it.

In late June 2025, it was reported to Mr. Borges that no verified audit or oversight mechanisms existed over the DOGE cloud environment set up outside of DIS control, and no one outside the former DOGE group had insight into code being executed against SSA's live production data.

v. DOGE Official Self-Authorizes a "Provisional Authorization to Operate" DOGE Cloud Environment Without Independent Security Controls

On July 15, 2025, Aram Moghaddassi authorized a "Provisional Authorization to Operate" apparently for the NUMIDENT cloud project stating, "I have determined the business need is higher than the security risk associated with this implementation and I accept all risks associated with this implementation and operation."[65] Mr. Borges reasonably believes this authorization to be an abuse of authority and to constitute gross mismanagement, substantial and specific threat to public health and safety, and potential violation of law as – in effect – Moghaddassi circumvented independent security monitoring and authorized himself to "assume the risk" of holding a copy of the American public's social security data in a potentially unsecured cloud environment. In reality, it is the American people who assume the risk.

As CDO, Mr. Borges' position requires full visibility into data access, data exchange, and cloud-based environments used for SSA production systems. He has not had such access regarding this cloud environment holding production data. Moreover, to Mr. Borges' knowledge, the three conditions identified in the risk assessment necessary to mitigate risk, namely: 1) that production data not be used, 2) that DIS be involved to ensure agency security policy is followed, and 3) that an ATO be obtained to ensure proper documentation of controls and risks, per FISMA, have not been met.

The creation of this environment has potentially violated multiple federal statutes. Under 44 U.S.C. § 3553(b), the Federal Information Security Modernization Act (FISMA) of 2014, federal agencies must implement security controls commensurate with the risk and magnitude of harm from unauthorized disclosure. By knowingly placing a High-Value Asset containing data on over 450 million people in an uncontrolled environment, the requestors, apparently

[64] Exhibit 2, p. 8
[65] Exhibit 8, p. 36

Moghaddassi and possibly others, violated statutory duties under FISMA. This data environment also potentially violated 5 U.S.C. § 552a(e)(1) of the Privacy Act, which requires agencies to maintain personal information with accuracy, relevance, timeliness, and completeness as necessary to assure fairness in determinations about individuals. Placing production NUMIDENT data in cloud environments without independent security controls violates these maintenance requirements. This action also potentially violated 18 U.S.C. § 1030, the Computer Fraud and Abuse Act, by facilitating unauthorized access to protected computer systems.

Further, Moghaddassi's self-authorization of risk acceptance potentially violated 44 U.S.C. § 3554(b), FISMA's requirements for continuous monitoring and risk management, by formally accepting risks that exceeded federal guidelines for protecting sensitive government information.

VI. Mr. Borges' Internal Protected Whistleblower Activity

In accordance with his statutory responsibilities at the Chief Data Officer for SSA, outlined in 44 U.S.C. § 3520, Mr. Borges has engaged in inquiries and reports regarding the concerns he has outlined above.

On August 6, 2025, Mr. Borges made internal disclosures to his superiors regarding the concerns outlined above. In that discussion, Mr. Borges commented that re-issuance of Social Security Numbers to all who possess one was a potential worst case outcome, and one of his superiors noted that possibility, underscoring the risk to the public.

On August 7, 2025, Mr. Borges sent an email requesting information about the concerns raised in this disclosure to officials in the Office of the Chief Information Security Officer, and on August 8, 2025 communicated the same request to officials in the Office of Systems Operations and Hardware Engineering, both within the OCIO.

On August 11, 2025, Mr. Borges contacted Edward Coristine, John Solly, and Mickie Tyquiengco, the Executive Officer in the OICO Front Office, to request information about data security concerns including:

- The safety of SSA datasets in the cloud, particularly the AWS based VPCs between June and July 2025, which would encompass the NUMIDENT cloud project initiated by John Solly on June 10, 2025;
- Security process and unauthorized data access, including write access, that did not follow standard protocols;
- Risk assessments; and
- Requests to bypass standard procedures, along with other specifications in his

request.[66]

That same day, in response to Mr. Borges' August 8, 2025 request for information about concerns raised, a CIO employee confirmed that while two cloud access accounts owned by Aaram Moghaddassi were created per SSA policy, they are not managed by the Division of Infrastructure Services (DIS), are self-administered, and include access to both test and live data environments.[67] Also on August 11, 2025 in response to the same August 7, 2025 request from Mr. Borges, another CIO employee provided the July 15, 2025 PATO and the June 25, 2025 approval by Russo of the NUMIDENT data transfer.

This information, while responsive to Mr. Borges' request for information regarding data security concerns, serves to support Mr. Borges' reasonable belief that the creation of the DOGE specific, self-administered cloud environment lacking independent security controls and hosting a copy of NUMIDENT constitutes an abuse of authority, gross mismanagement, substantial and specific threat to public health and safety, and potentially violation of law, rule, or regulation.

Moreover, to date, Mr. Borges has not received a response to his August 7, 2025 request for information from Coristine, Solly, and Tyquiengco. Nor has he received information to indicate that the cloud environment hosting the American public's NUMIDENT data is protected by best practice and industry standard independent security controls. This leaves Mr. Borges with the reasonable belief that the NUMIDENT data is at risk of exposure, and without information necessary to effectuate his responsibilities as CDO.

Furthermore, Mr. Borges is aware that the Office of General Counsel has advised employees not to respond to his inquiries.[68] Such restriction on information to the CDO puts Mr. Borges in an untenable position inhibiting his ability to effectuate the responsibilities of his role.

VII. Conclusion

Mr. Borges' disclosures establish escalating federal law violations at the Social Security Administration involving the unauthorized handling of sensitive data affecting over 300 million Americans and millions of additional members of the American public. The violations progressed from emergency circumvention of court orders in March 2025 to systematic institutional approval of high-risk activities involving sensitive public data by July 2025.

Mr. Borges stands ready to meet with oversight entities and members of Congress to discuss his disclosures. We call on Congress and the Office of Special Counsel to engage in swift oversight to investigate Mr. Borges' disclosures and ensure that the security of data of millions

[66] Exhibit 5, p. 29
[67] Exhibit 6, pp. 31-32
[68] Exhibit 6, pp. 31-32