

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Howard Lutnick  
Secretary  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Washington, DC 20230

Dear Secretary Lutnick:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Commerce (DOC) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the DOC have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the DOC or DOGE is covered by the Advancing AI Act, and the DOC and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the DOC, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the DOC in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing DOC spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the DOC is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where DOC data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing DOC data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the DOC's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Howard Lutnick  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Kristi Noem  
Secretary  
U.S. Department of Homeland Security  
301 7th Street, SW  
Washington, DC 20528

Dear Secretary Noem:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Homeland Security (DHS) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by DHS have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by DHS or DOGE is covered by the Advancing AI Act, and DHS and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).



At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by DHS, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside DHS in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing DHS spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of DHS is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where DHS data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing DHS data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that DHS's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Pete Hegseth  
Secretary  
U.S. Department of Defense  
1400 Defense Pentagon  
Washington, DC 20301

Dear Secretary Hegseth:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Defense (DOD) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the DOD have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the DOD or DOGE is covered by the Advancing AI Act, and the DOD and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the DOD, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the DOD in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing DOD spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the DOD is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where DOD data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;



5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing DOD data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the DOD's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Pete Hegseth  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Chris Wright  
Secretary  
U.S. Department of Energy  
1000 Independence Avenue, SW  
Washington, DC 20585

Dear Secretary Wright:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Energy (DOE) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the DOE have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the DOE or DOGE is covered by the Advancing AI Act, and the DOE and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the DOE, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the DOE in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing DOE spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the DOE is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where DOE data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing DOE data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the DOE's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Chris Wright  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.



# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Doug Burgum  
Secretary  
U.S. Department of the Interior  
1849 C Street, NW  
Washington, DC 20240

Dear Secretary Burgum:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of the Interior (DOI) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the DOI have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the DOI or DOGE is covered by the Advancing AI Act, and the DOI and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the DOI, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the DOI in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing DOI spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the DOI is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where DOI data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing DOI data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the DOI's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Pamela Bondi  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington, DC 20530

Dear Attorney General Bondi:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Justice (DOJ) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the DOJ have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the DOJ or DOGE is covered by the Advancing AI Act, and the DOJ and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).



At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the DOJ, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the DOJ in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing DOJ spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the DOJ is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where DOJ data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing DOJ data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the DOJ's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Pamela Bondi  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

Mr. Vince Micone  
Acting Secretary  
U.S. Department of Labor  
200 Constitution Avenue, NW  
Washington, DC 20001

Dear Acting Secretary Micone:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Labor (DOL) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the DOL have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the DOL or DOGE is covered by the Advancing AI Act, and the DOL and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the DOL, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the DOL in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing DOL spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the DOL is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where DOL data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;



5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing DOL data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the DOL's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

Mr. Vince Micone

Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Sean Duffy  
Secretary  
U.S. Department of Transportation  
1200 New Jersey Avenue, SE  
Washington, DC 20590

Dear Secretary Duffy:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Transportation (DOT) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the DOT have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the DOT or DOGE is covered by the Advancing AI Act, and the DOT and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the DOT, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the DOT in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing DOT spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the DOT is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where DOT data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing DOT data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the DOT's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.



# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Linda McMahon  
Secretary  
U.S. Department of Education  
400 Maryland Avenue, SW  
Washington, DC 20202

Dear Secretary McMahon:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Education (ED) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by ED have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by ED or DOGE is covered by the Advancing AI Act, and ED and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at ED. On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by ED, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside ED in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing ED spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of ED is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where ED data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing ED data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that ED's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Linda McMahon

Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Lee Zeldin  
Administrator  
U.S. Environmental Protection Agency  
1200 Pennsylvania Avenue, NW  
Washington, DC 20460

Dear Administrator Zeldin:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Environmental Protection Agency (EPA) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the EPA have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the EPA or DOGE is covered by the Advancing AI Act, and the EPA and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).



At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the EPA, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the EPA in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing EPA spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the EPA is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where EPA data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing EPA data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the EPA's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Lee Zeldin

Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

Mr. Stephen Ehikian  
Acting Administrator  
U.S. General Services Administration  
1800 F Street, NW  
Washington, DC 20405

Dear Acting Administrator Ehikian:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the General Services Administration (GSA) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the GSA have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the GSA or DOGE is covered by the Advancing AI Act, and the GSA and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the GSA, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the GSA in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing GSA spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the GSA is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where GSA data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;



5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing GSA data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the GSA's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

Mr. Stephen Ehikian

Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Robert F. Kennedy  
Secretary  
U.S. Department of Health and Human Services  
200 Independence Avenue, SW  
Washington, DC 20201

Dear Secretary Kennedy:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Health and Human Services (HHS) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by HHS have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by HHS or DOGE is covered by the Advancing AI Act, and HHS and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by HHS, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside HHS in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing HHS spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of HHS is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where HHS data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing HHS data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that HHS's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Robert F. Kennedy  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.



# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Scott Turner  
Secretary  
U.S. Department of Housing and Urban Development  
451 7th Street, SW  
Washington, DC 20410

Dear Secretary Turner:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Housing and Urban Development (HUD) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by HUD have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by HUD or DOGE is covered by the Advancing AI Act, and HUD and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by HUD, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside HUD in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing HUD spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of HUD is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where HUD data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing HUD data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that HUD's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Scott Turner

Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

Ms. Janet Petro  
Acting Administrator  
National Aeronautics and Space Administration  
300 E Street, SW  
Washington, DC 20024

Dear Acting Administrator Petro:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the National Aeronautics and Space Administration (NASA) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by NASA have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by NASA or DOGE is covered by the Advancing AI Act, and NASA and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).



At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by NASA, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside NASA in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing NASA spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of NASA is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where NASA data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing NASA data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that NASA's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

Ms. Janet Petro

Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable David A. Wright  
Chairman  
Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852

Dear Chairman Wright:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Nuclear Regulatory Commission (NRC) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the NRC have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the NRC or DOGE is covered by the Advancing AI Act, and the NRC and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the NRC, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the NRC in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing NRC spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the NRC is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where NRC data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;



5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing NRC data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the NRC's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable David A. Wright  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

Dr. Sethuraman Panchanathan  
Director  
National Science Foundation  
2415 Eisenhower Avenue  
Alexandria, VA 22314

Dear Director Panchanathan:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the National Science Foundation (NSF) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the NSF have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the NSF or DOGE is covered by the Advancing AI Act, and the NSF and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the NSF, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the NSF in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing NSF spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the NSF is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where NSF data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing NSF data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the NSF's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.



# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

Mr. Charles Ezell  
Acting Director  
Office of Personnel Management  
1900 E Street, NW  
Washington, DC 20415

Dear Acting Director Ezell:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Office of Personnel Management (OPM) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by OPM have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by OPM or DOGE is covered by the Advancing AI Act, and OPM and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by OPM, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside OPM in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing OPM spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of OPM is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where OPM data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing OPM data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that OPM's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

Mr. Charles Ezell

Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074  
MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Kelly Loeffler  
Administrator  
U.S. Small Business Administration  
409 3rd Street, SW  
Washington, DC 20416

Dear Administrator Loeffler:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Small Business Administration (SBA) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the SBA have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the SBA or DOGE is covered by the Advancing AI Act, and the SBA and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).



At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the SBA, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the SBA in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing SBA spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the SBA is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where SBA data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing SBA data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the SBA's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Kelly Loeffler  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

Mr. Leland Dudek  
Acting Commissioner  
U.S. Social Security Administration  
1300 D Street, SW  
Washington, DC 20254

Dear Acting Commissioner Dudek:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Social Security Administration (SSA) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the SSA have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the SSA or DOGE is covered by the Advancing AI Act, and the SSA and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the SSA, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the SSA in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing SSA spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the SSA is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where SSA data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;



5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing SSA data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the SSA's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

Mr. Leland Dudek

Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Marco Rubio  
Secretary  
U.S. Department of State  
2201 C Street, NW  
Washington, DC 20451

Dear Secretary Rubio:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of State (State) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by State have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by State or DOGE is covered by the Advancing AI Act, and State and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by State, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside State in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing State spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of State is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where State data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing State data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that State's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Marco Rubio  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.



# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Scott Bessent  
Secretary  
U.S. Department of the Treasury  
1500 Pennsylvania Avenue, NW  
Washington, DC 20220

Dear Secretary Bessent:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of the Treasury (Treasury) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the Treasury have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the Treasury or DOGE is covered by the Advancing AI Act, and the Treasury and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the Treasury, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the Treasury in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing Treasury spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the Treasury is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where Treasury data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team

members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing Treasury data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the Treasury's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Marco Rubio  
Acting Administrator  
U.S. Agency for International Development  
1300 Pennsylvania Avenue, NW  
Washington, DC 20004

Dear Acting Administrator Rubio:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Agency for International Development (USAID) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by USAID have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by USAID or DOGE is covered by the Advancing AI Act, and USAID and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).



At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by USAID, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside USAID in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing USAID spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of USAID is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where USAID data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing USAID data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that USAID's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

The Honorable Marco Rubio  
Page 6

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074  
MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Brooke Rollins  
Secretary  
U.S. Department of Agriculture  
1400 Independence Avenue, SW  
Washington, DC 20250

Dear Secretary Rollins:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Agriculture (USDA) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the USDA have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the USDA or DOGE is covered by the Advancing AI Act, and the USDA and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the USDA, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the USDA in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing USDA spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the USDA is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where USDA data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team



members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing USDA data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the USDA's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

March 12, 2025

The Honorable Doug A. Collins  
Secretary  
U.S. Department of Veterans Affairs  
810 Vermont Avenue, NW  
Washington, DC 20420

Dear Secretary Collins:

I write with serious concerns about the use of unapproved, third-party artificial intelligence (AI) software employed by members of the U.S. DOGE Service (DOGE) at federal agencies. The American people entrust the federal government with sensitive personal information related to their health, finances, and other biographical information on the basis that this information will not be disclosed or improperly used without their consent, including through the use of an unapproved and unaccountable third-party AI software. I urgently request documentation to demonstrate that any potential use of AI software at the Department of Veterans Affairs (VA) complies with federal law, protects Americans' sensitive and private data, and does not financially benefit Elon Musk.

Federal agencies are bound by multiple statutory requirements in their use of AI software. The Federal Risk and Authorization Management Program (FedRAMP) is the federal government's "authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information"—in short, FedRAMP ensures that the whole-of-government uses secure cloud services.<sup>1</sup> Failing to ensure that AI vendors used by the VA have adequate FedRAMP approval risks violating the Privacy Act of 1974, the Federal Information Security Management Act, and the E-Government Act of 2002.<sup>2</sup> Moreover, the Advancing American AI Act requires agencies to keep an inventory of "current and planned uses" of AI and for those inventories to be made public.<sup>3</sup> Any use of AI by the VA or DOGE is covered by the Advancing AI Act, and the VA and DOGE must fully comply with this legal obligation for public transparency.<sup>4</sup>

---

<sup>1</sup> FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Announces the Passing of the FedRAMP Authorization Act!* (Jan. 11, 2025) (online at [www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/](http://www.fedramp.gov/blog/2023-01-11-announces-passing-fedramp-auth-act/)).

<sup>2</sup> Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

<sup>3</sup> 40 U.S.C. § 11301.

<sup>4</sup> 40 U.S.C. § 11301; *see* 44 U.S.C. § 3502 (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory

Illustrative of my concerns is the ongoing DOGE-related activity at the Department of Education (ED). On February 6, 2025, the *Washington Post* reported that members of the DOGE team assigned to ED had begun probing internal datasets using AI software. These datasets contain sensitive internal financial data as well as the personally identifiable information of people who manage grants. The reporting further detailed that the DOGE team is feeding this private information into AI software accessed through a private cloud computing service as a method of examining ED disbursements.<sup>5</sup> In one reported incident, DOGE team members allegedly uploaded agency staffing and expenditure reports into an AI platform and asked the algorithm to identify “inefficiencies.”<sup>6</sup> After tasking the AI to suggest ways to cut ED’s budget by over 50%, DOGE operatives began drafting proposals to gut the agency.<sup>7</sup>

On February 9, 2025, U.S. government IP addresses were linked to Inventory.ai, an AI product designed for supply chain management.<sup>8</sup> Further analysis found indications of a “massive firehose of data being sent to the AI company’s servers,” likely connected to the disclosure of ED data to the company by DOGE team members.<sup>9</sup> The AI vendor, Inventory.ai, reportedly used by the DOGE team has not been approved for federal cloud use through the FedRAMP process.<sup>10</sup> These actions demonstrate reckless AI misuse, blatant disregard for data privacy, and a severe failure to maintain the cybersecurity of federal systems.

---

agency.”)

<sup>5</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)).

<sup>6</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at [www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676](https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676)).

<sup>7</sup> *Id.*

<sup>8</sup> *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); *How It Works*, Inventory.ai (accessed Feb. 12, 2025) (online at [www.inventory.ai/how-it-works](https://www.inventory.ai/how-it-works)).

<sup>9</sup> *Elon Musk’s DOGE is Feeding Sensitive Federal Data into AI to Target Cuts*, The Washington Post (Feb. 6, 2025) (online at [www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/](https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education/)); *DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever*, Cyber-Intelligence Brief (Feb. 9, 2025) (online at <https://cyberintel.substack.com/p/doge-exposes-once-secret-government?triedRedirect=true>); Shodan.io, 18.253.166.131 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.166.131](https://www.shodan.io/host/18.253.166.131)); Shodan.io, 182.30.117.29 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.117.29](https://www.shodan.io/host/182.30.117.29)); Shodan.io, 182.30.1.117 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.1.117](https://www.shodan.io/host/182.30.1.117)); Shodan.io, 182.30.154.252 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/182.30.154.252](https://www.shodan.io/host/182.30.154.252)); Shodan.io, 18.254.229.158 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.229.158](https://www.shodan.io/host/18.254.229.158)); Shodan.io, 18.253.160.247 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.253.160.247](https://www.shodan.io/host/18.253.160.247)); Shodan.io, 18.254.175.18 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.175.18](https://www.shodan.io/host/18.254.175.18)); Shodan.io, 18.254.191.201 (accessed Feb. 27, 2025) (online at [www.shodan.io/host/18.254.191.201](https://www.shodan.io/host/18.254.191.201)).

<sup>10</sup> See FedRAMP Program Management Office, U.S. General Services Administration, *FedRAMP Marketplace* (accessed Feb. 26, 2025) (online at <https://marketplace.fedramp.gov/products>).

At ED, the DOGE team reportedly accessed incredibly sensitive data that likely includes the personally identifiable information of as many as 43.5 million people connected to federal student aid programs.<sup>11</sup> ED collects personally identifiable information throughout the student aid process, including a student or borrower's name, Social Security number (SSN), date of birth, student loan account information, contact information, driver's license number, and financial information.<sup>12</sup> Due to the opaque and frenetic pace at which DOGE seems to be operating, I am deeply concerned that students', parents', spouses', family members' and all other borrowers' sensitive information is being handled by secretive members of the DOGE team for unclear purposes and with no safeguards to prevent disclosure or improper, unethical use. If sensitive personnel files were uploaded to AI models, those files may now be accessible to third parties, including foreign adversaries.<sup>13</sup> Moreover, concerns that Elon Musk is using sensitive government data to "supercharge" his proprietary AI model "Grok" developed by xAI raise the possibility that Musk is leveraging access to sensitive government data for commercial advancement and private enrichment.<sup>14</sup>

The use of AI to evaluate sensitive data is fraught with serious hazards beyond improper disclosure: the inputs used and the parameters selected for analysis may be flawed, errors may be introduced through the design of the AI software, and staff may misinterpret AI recommendations, among other concerns. Without clear purpose behind the use of AI, guardrails to ensure appropriate handling of data, and adequate oversight and transparency, the application of AI is dangerous and potentially violates federal law.<sup>15</sup>

To better understand how DOGE is using the private data of millions of Americans, I request that you provide the following information by March 26, 2025:

1. A detailed and comprehensive explanation of the legal authorities used by Elon Musk and/or DOGE team members to access and analyze data stored by the VA, including but not limited to any associated System of Records Notice;
2. A detailed and complete list of the sources of data collected, analyzed, or otherwise used by Elon Musk, DOGE team members, or any representatives of the Administration from outside the VA in connection with AI;

---

<sup>11</sup> Office of Federal Student Aid, U.S. Department of Education, *Federal Student Loan Portfolio: By Location* (Jan. 19, 2024) (online at <https://studentaid.gov/data-center/student/portfolio>).

<sup>12</sup> Office of Federal Student Aid, U.S. Department of Education, *Privacy Policy for StudentAid.gov* (April 26, 2024) (online at <https://studentaid.gov/notices/privacy>).

<sup>13</sup> *DOGE Workers Accused of Dumping Sensitive Data into AI, Asking Software to Slash Education Department Budget*, International Business Times (Feb. 6, 2025) (online at <https://www.ibtimes.com/doge-workers-accused-dumping-sensitive-data-ai-asking-software-slash-education-department-budget-3762676>).

<sup>14</sup> *What's Elon Musk Doing With Your Data?* Politico (Feb. 20, 2025) (online at <https://www.politico.com/news/2025/02/20/musk-data-ai-00205259>).

<sup>15</sup> See, e.g., 5 U.S.C. § 552a(i)(1); see also 26 U.S.C. § 7213 (a)(1).

3. A detailed and comprehensive description of the privacy protections employed by Elon Musk, DOGE team members, or any representatives of the Administration in connection with Trump Administration efforts to analyze spending with the use of AI, including all data anonymization policies, practices, and procedures and any associated Privacy Impact Assessments;
4. A detailed and comprehensive description of all AI software employed since January 20, 2025, by Elon Musk and/or DOGE team members in analyzing VA spending, data, and other records, including:
  - a. The name of the AI software, the version used, the developer and/or creator of the AI software, where the computing takes place, and any substantial modifications made to the AI software that could impact the analysis, detection, identification, or any other outcomes rendered by the program;
  - b. The data used to develop the AI algorithm, including the training, validation, and testing data sets;
  - c. The definitions and parameters used by Elon Musk, DOGE team members, or any representatives of the Administration to assess whether a contract, expenditure, program, or personnel of the VA is deemed waste, fraud, or abuse, or is otherwise identifiable for potential elimination;
  - d. The information inputs the AI software requires for analysis;
  - e. The degree to which a human supervisor reviews, approves, or denies a disbursement, contract, program, or employee upon identification by an AI software program for potential elimination;
  - f. The information connected to an analyzed disbursement, contract, program, or employee that is displayed to a human reviewer upon identification of potential waste, fraud, or abuse by an AI algorithm;
  - g. The results and any analysis of results of testing for errors or bias in identification, analysis, or detection of waste, fraud, or abuse;
  - h. Where VA data is being stored by members of DOGE or any representative of the Administration outside of the agency if not in the same systems used on January 19, 2025, and whether any copies of the data have been made and stored elsewhere;
  - i. All records, logs, code, certificates, and configurations for all federal IT assets, databases, or repositories accessed by Elon Musk, DOGE team members, and associated persons in training or deploying new AI software;

5. A detailed and complete description of any assessment of risks of the use of AI in connection with analyzing VA data, contracts, expenditures, programs, or personnel, including any concerns raised by Federal workers that such actions by Elon Musk, DOGE team members, or the Administration violate the Privacy Act, FISMA, the Advancing American AI Act, or any other law, or otherwise negatively affect the security of Americans' private information;
6. A detailed and complete list of the personnel, processes, and evaluation criteria being used to make determinations on the continuation or elimination of contracts, disbursements, grants, or other programs after being identified by an AI program for potential elimination, as well as any analyses undertaken by any individuals to determine which of the AI-identified contracts, expenditures, programs, or personnel to freeze or cut;
7. A detailed and comprehensive description of the adjudication process for contract, disbursement, or employee termination decisions made pursuant to identification by an AI algorithm for elimination;
8. A detailed response to concerns that the VA's data will be used to train, test, or otherwise develop an AI algorithm for private use and personal enrichment, such as but not limited to the "Grok" AI program created by Elon Musk-owned xAI.
9. A complete list of all individuals involved in both the policy decisions and technical planning associated with the feeding of sensitive Federal data to AI technology from January 20, 2025, to present, including:
  - a. Individuals involved in plans to use AI technology to cut payments to Americans or associated with programs for Americans;
  - b. Individuals involved in plans to collect and feed government contract data through AI software, including any concerns raised or steps taken to mitigate Elon Musk's related potential conflicts of interest;
10. All communication or correspondence regarding the legality of freezes and cuts of AI-identified expenditures, programs, or personnel, as well as the harms to the American people of such freezes and cuts; and,
11. A complete list of all individuals who managed or accessed federal data in the process of feeding it through AI technology, including whether such individuals were federal employees at the time of their data management or access and, if so, under what authority they were hired and what background investigation and clearance processes they underwent as part of the hiring process.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at

“any time” under House Rule X. The Committee has jurisdiction over the “overall economy, efficiency, and management of government operations and activities, including Federal procurement.”<sup>16</sup> Responses to this request for information will inform necessary legislative reforms on the topics covered in this letter. If you have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Ranking Member

cc: The Honorable James Comer, Chairman

---

<sup>16</sup> House rule X, clause 1.