

EXHIBIT 3

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

AMERICAN FEDERATION OF LABOR
AND CONGRESS OF INDUSTRIAL
ORGANIZATIONS, *et al.*,

Plaintiffs,

v.

DEPARTMENT OF LABOR, *et al.*,

Defendants.

Case No. 1:25-cv-00339-JDB

Judge John D. Bates

**DEFENDANTS' OBJECTIONS AND RESPONSES TO
PLAINTIFFS' REQUESTS FOR EXPEDITED DISCOVERY, INCLUDING
SUPPLEMENTAL RESPONSES**

Pursuant to Federal Rules of Civil Procedure 26, 30, 33, and 34; and to the Local Rules of the United States District Court for the District of Columbia, Defendants—the U.S. Department of Labor, Secretary of Labor Lori Chavez-DeRemer, the U.S. Department of Health and Human Service, Secretary of Health and Human Services Robert F. Kennedy, Jr., the Consumer Financial Protection Bureau, Acting CFPB Director Russell Vought, the U.S. Digital Service (U.S. DOGE Service), and U.S. DOGE Service Temporary Organization—provides the following responses to Plaintiffs' discovery requests, as modified by the Court's March 19, 2025 Memorandum Opinion and Order, ECF No. 71, and March 31, 2025 Memorandum Opinion and Order, ECF No. 75.

I. GENERAL OBJECTIONS

1. The following general objections apply to, and are incorporated in, each individual response.

2. Defendants object to providing any discovery at all at this time, as Defendants have a pending motion to dismiss that the Court has not yet decided; Defendants have not answered the amended complaint; there has been no conference of the parties, as required by Rule 26(f) and Local Civil Rule 16.3(b); and as to Plaintiffs' Administrative Procedure Act claims, Defendants have yet to produce an administrative record.

3. Defendants object to the definitions in Plaintiffs' requests to the extent that the definitions conflict with or purport to expand upon the Defendants' obligations under the Federal Rules of Civil Procedure, the Local Rules for the United States District Court for the District of Columbia, or the Court's orders for discovery, *see* ECF Nos. 48, 71, 75.

4. Defendants object to each and every request to the extent that it is deemed to require disclosure of matters subject to the attorney-client privilege, the attorney work product doctrine, other applicable privileges, or any statutory or regulatory restriction on disclosure.

5. Defendants object to the term "DOGE Employee," as used throughout Plaintiffs' discovery requests, because the phrase "works for DOGE" and "otherwise works for DOGE" in Plaintiffs' definition of that term are vague and ambiguous. Defendants recognize the Court's clarification that these terms include members of DOGE Teams, as defined in Executive Order 14,158, 90 Fed. Reg. 8441, § 3(c), "that the defendant agencies have onboarded for the purpose of carrying out the DOGE Agenda, including those the agencies have directly hired or received as detailees[.]" after January 20, 2025. ECF No. 75 at 5.

6. Defendants object to the term "Sensitive Systems," as used throughout Plaintiffs' discovery requests, because the phrase "system of records" in Plaintiffs' definition of "Sensitive Systems" is undefined and therefore vague and ambiguous. Defendants will interpret the term "system of records" as it is used by the Privacy Act of 1974, 5 U.S.C. § 552a.

7. Defendants object to the term “Access,” as used throughout Plaintiffs’ discovery requests, because the phrase “directly review records in an agency system” in Plaintiffs’ definition of that term is vague and ambiguous. Defendants further object that the terms “directly,” “records,” and “system” are undefined and ambiguous. Defendants will interpret the phrase “directly” in its usual sense, and understand “records” and “system” as those terms are used in the Privacy Act, 5 U.S.C. § 552a.

8. Defendants object to the term “records,” as used throughout Plaintiffs’ discovery requests, as vague and ambiguous. Defendants will interpret the terms “record” and “records” as used in the Privacy Act, 5 U.S.C. § 552a.

9. Defendants reserve the right to amend, supplement, or alter these objections at any time.

10. Nothing contained in the following specific objections and responses constitutes a waiver of any applicable objection or privilege as to the requested discovery.

II. RESERVATION OF RIGHTS AND OBJECTIONS

The foregoing general objections and the following specific objections and responses are based on the Defendants’ interpretation of the Plaintiffs’ interrogatories, requests for production, and notices of deposition pursuant to Rule 30(b)(6), and on information reasonably available to Defendants as of today. Defendants reserve the right to supplement these objections or responses if the plaintiffs purport to interpret their requests differently than Defendants or if Defendants discover new information supporting additional objections or responses. Defendants also reserve the right to object to the admissibility of any information contained herein on the grounds of relevance, proportionality, accessibility, materiality, or any other appropriate ground.

III. SPECIFIC OBJECTIONS & RESPONSES TO INTERROGATORIES

INTERROGATORY NO. 1: Identify each DOGE Employee who has Accessed, has been granted permission to Access, or has a pending request to Access, any Sensitive Systems at Defendant Agencies, and for each, please provide:

- a. The names of each Sensitive System that the DOGE Employee has been granted Access to;
- b. The date that the DOGE Employee was granted permission to Access Sensitive Systems at Defendant Agencies;
- c. The identity of any employee of Defendant Agencies who authorized the DOGE Employee to Access Sensitive Systems;
- d. The name and description of each training program the DOGE Employee completed prior to being granted Access to each Sensitive System;
- e. A summary of the actual usage of each Sensitive System by the DOGE Employee, including a description of the records reviewed, the purpose for which they were reviewed, any restrictions on the DOGE Employee's Access, and whether any records were modified, copied, shared, or removed from Defendant Agencies' systems, and, if so, the identity of any person(s) with whom those records have been shared;
- f. The name and a summary of the function of any software installed by, or caused to be installed by, the DOGE Employee on Agency networks or systems;
- g. The names of each Sensitive System to which DOGE Employees have been denied access by Defendant Agencies; and

- h. The number of federal agencies that the DOGE Employee is concurrently detailed to or otherwise employed by.

Objections: Defendants object that these requests are not relevant to Plaintiffs' forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.' Mot. for Reconsideration, ECF No. 51. Defendants object that these requests are premature, as set forth in General Objection 2. Defendants further object to this request to the extent it calls for privileged information, as set forth in General Objection 4. Defendants further object to the term "DOGE Employee," as set forth in General Objection 5. Defendants further object to the term "Sensitive Systems," as set forth in General Objection 6. Defendants further object to the terms "Access" and "Accessed," as set forth in General Objection 7. Defendants further object to the terms "record" and "records," as set forth in General Objection 8. Defendants further object to the extent Plaintiffs seek information about individuals who are no longer detailed to, or employed at, one of the Agency Defendants. Defendants further object to subpart e on the grounds that "actual usage" is vague and ambiguous, and that providing a summary of all usage of each Sensitive System by any DOGE Employee, as described therein, is overbroad, unduly burdensome, and disproportionate to the needs of the case. Defendants further object that the term "system" in subpart e and subpart f is undefined, and therefore vague and ambiguous. Defendants further object that the term "networks" in subpart f is vague and ambiguous.

Subject to, and without waiving, the General and Specific objections asserted, Defendant Agencies answer the interrogatory as follows:

A. Response as to the U.S. Department of Health and Human Services

HHS's response reflects its current knowledge as of the date of service of this interrogatory. HHS reserves the right to amend this response to the extent it learns of additional facts that might alter or

change any of the information provided below. The individuals listed below have an employment relationship with the U.S. DOGE Service (USDS) beginning on January 20, 2025 or after.

Amy Gleason

Amy Gleason is the only HHS employee that is also an employee of DOGE who has been granted permission to access sensitive systems at the agency.

Ms. Gleason was granted read-only access to the Centers for Medicare and Medicaid Services (CMS) Acquisition Lifecycle Modernization (CALM) contract writing system on February 24, 2025, by the Chief Information Officer, CMS Office of Information Technology. Ms. Gleason has accessed CALM in furtherance of Executive Order 14,158 titled “Establishing and Implementing the President’s ‘Department of Government Efficiency’” (DOGE) (hereinafter “the DOGE EO”). The DOGE EO directs the USDS to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Ms. Gleason has not modified, copied, shared, or removed any records from any of these systems.

There are currently no pending requests to grant Ms. Gleason access to other sensitive systems at HHS or CMS, nor has Ms. Gleason been denied access to any systems at HHS or CMS.

As part of her onboarding process at HHS/CMS, Ms. Gleason completed computer-based training (CBT) on the proper management of CMS systems and operating within the CMS network; HHS Information Systems Security and Privacy Awareness Training; acknowledged the Rules of Behavior for General Users v. 3.0; and acknowledged under penalty of perjury that she will adhere to the Privacy Act and other HHS rules of behavior upon receipt of her HHS access card.

Ms. Gleason has neither installed nor requested to be installed any unapproved software on HHS or CMS networks or systems.

Luke Farritor

Luke Farritor is an employee of the General Services Administration (GSA) and has been detailed to HHS since January 21, 2025, in furtherance of the DOGE EO. Mr. Farritor is also detailed to USDS

from GSA.

Mr. Farritor has been granted permission to access the following Sensitive Systems at HHS:

1. Payment Management System (PMS) on January 22, 2025, by the Chief Technology Officer, Program Support Center;
2. GrantSolutions on January 27, 2025, by the Director, Security and Data Project Management Office, HHS Office of Grants;
3. Healthcare Integrated General Ledger Accounting System (HIGLAS) on January 31, 2025 by the Chief Information Officer, CMS Office of Information Technology;
4. HHS Consolidated Acquisition System (HCAS) on January 29, 2025, by the Executive Director, Strategic Programs and Business Systems at the Office of the Assistant Secretary for Financial Resources (ASFR);
5. CMS Acquisition Lifecycle Modernization (CALM) system on February 3, 2025, by the Chief Information Officer, CMS Office of Information Technology;
6. Integrated Data Repository (IDR) at CMS on February 18, 2025, by the Chief Information Officer, CMS Office of Information Technology;
7. NIH's grants management system (eRA) on January 27, 2025, by the NIH Office of the Chief Information Officer;
8. Enterprise Human Capital Management System (EHCM) on February 28, 2025, by the Human Resources Information System Security Officer;
9. Integrated Contracts Expert (ICE) system at CDC on January 30, 2025, by the CDC's Office of the Chief Information Officer;
10. Acquisition Performance and Execution (APEX) system at CDC on February 4, 2025, by the CDC's Office of the Chief Information Officer;
11. NIH Business System EBS and PRISM systems on February 28, 2025, by the NIH's Office of the Chief Information Officer; and

12. Grants.gov on March 21, 2025, by the Assistant Secretary for Financial Resources (ASFR).

Mr. Farritor has been granted administrator privileges for PMS, EHCM, Grants.gov, and HCAS by the system owners of these systems, otherwise his access to the other listed systems above is read-only.

Mr. Farritor accessed EBS, PMS, Grants.gov, and eRA in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Mr. Farritor has not modified, copied and shared with any unauthorized users, or removed any records from any of these systems.

There are currently no pending requests to grant Mr. Farritor access to other sensitive systems at HHS, nor has Mr. Farritor been denied access to any systems at HHS.

As part of his onboarding process at HHS, Mr. Farritor acknowledged the Rules of Behavior for General Users; the Rules of Behavior for Privileged Users; a security briefing for HIGLAS; completed IDR computer-based training; and completed Cybersecurity training. In addition, Mr. Farritor completed Information Security and Information Management Training at NIH.

Mr. Farritor has neither installed nor requested to be installed any unapproved software on HHS networks or systems. Mr. Farritor has been involved in standard software development activities inside the HHS internal cloud environment.

Edward Coristine

Edward Coristine is an employee of the General Services Administration (GSA) and has been detailed to HHS since March 5, 2025, in furtherance of the DOGE EO. Mr. Coristine is also detailed to USDS from GSA.

Mr. Coristine has been granted permission to access the following Sensitive Systems at HHS:

1. Healthcare Integrated General Ledger Accounting System (HIGLAS) on March 5, 2025, by the Chief Information Officer, CMS Office of Information Technology;
2. Integrated Data Repository (IDR) at CMS on March 11, 2025, by the Chief Information Officer, CMS Office of Information Technology; and

3. CMS Acquisition Lifecycle Modernization (CALM) contract writing system on March 5, 2025, by the Chief Information Officer, CMS Office of Information Technology.

Mr. Coristine was granted read-only access to the above-listed systems in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Mr. Coristine's access to the above-referenced systems has been disabled. Mr. Coristine has not modified, copied and shared with unauthorized users, or removed any records from the PMS system.

Mr. Coristine has not been granted access to any other HHS systems. In addition, there are currently no pending requests to grant Mr. Coristine access to other sensitive systems at HHS, nor has Mr. Coristine been denied access to any systems at HHS.

As part of his onboarding process at HHS, Mr. Coristine acknowledged the Rules of Behavior for General Users, and completed Cybersecurity training.

Mr. Coristine has neither installed nor requested to be installed any unapproved software on HHS networks or systems. Mr. Coristine has been involved in standard software development activities inside the HHS internal cloud environment.

Marko Elez

Marko Elez is an employee of the Department of Labor (DOL) and has been detailed to HHS since March 5, 2025, in furtherance of the DOGE EO. Mr. Coristine is also detailed to USDS from DOL.

Mr. Elez has been granted permission to access the following Sensitive Systems at HHS:

1. National Directory of New Hires (NDNH) database on March 6, 2025, by the Administration for Children and Families (ACF) Chief Technology Officer;
2. Healthcare Integrated General Ledger Accounting System (HIGLAS) on March 5, 2025, by the Chief Information Officer, CMS Office of Information Technology;
3. Integrated Data Repository (IDR) at CMS on March 5, 2025, by the Chief Information Officer, CMS Office of Information Technology; and

4. CMS Acquisition Lifecycle Modernization (CALM) contract writing system on March 5, 2025, by the Chief Information Officer, CMS Office of Information Technology.

Mr. Elez was granted read-only access to the above-listed systems in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Mr. Elez's access to the above-referenced CMS systems has been disabled. Mr. Elez has not modified, copied and shared with any unauthorized users, or removed any records from any of the systems he has actually accessed.

There are currently no pending requests to grant Mr. Elez access to other sensitive systems at HHS, nor has Mr. Elez been denied access to any systems at HHS.

As part of his onboarding process at HHS, Mr. Elez acknowledged the Rules of Behavior for General Users, the Rules of Behavior for the Office of Child Support Enforcement, completed Cybersecurity training, and received training from the Office of Child Support Services on navigating the screens to get to the NDNH database.

Mr. Elez has neither installed nor requested to be installed any software on HHS networks or systems.

Kyle Schutt

Kyle Schutt is an employee of the General Services Administration (GSA) and has been detailed to the Administration for Children and Families (ACF) at HHS since March 14, 2025, in furtherance of the DOGE EO. Mr. Schutt is also detailed to USDS from GSA.

Mr. Schutt has been granted read-only access to the Unaccompanied Alien Children (UAC) Portal on March 21, 2025, by the ACF Chief Technology Officer. Mr. Schutt was granted read-only access to the UAC Portal in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Mr. Schutt has not modified, copied and shared with any unauthorized users, or removed any records from the UAC Portal.

Mr. Schutt has not been granted access to any other HHS systems. In addition, there are currently

no pending requests to grant Mr. Schutt access to other sensitive systems at HHS, nor has Mr. Schutt been denied access to any systems at HHS.

As part of his onboarding process at HHS, Mr. Schutt acknowledged the Rules of Behavior for General Users, Rules of Behavior of Privilege Users, and completed Cybersecurity training. Mr. Schutt has neither installed nor requested to be installed any software on HHS networks or systems.

HHS's FIRST SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 1 (April 4, 2025):

HHS's response reflects its current knowledge as of the date of service of this interrogatory. HHS reserves the right to amend this response to the extent it learns of additional facts that might alter or change any of the information provided below.

Luke Farritor

Mr. Farritor has modified Grants.gov by restricting access to certain accounts and removing Notices of Funding Opportunity (NOFO).

Mr. Farritor accessed HCAS in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity.

Mr. Farritor's access to HCAS has been deactivated.

Edward Coristine

Mr. Coristine was not granted access to the PMS system and therefore the statement in the previous response that he "has not modified, copied and shared with unauthorized users, or removed any records from the PMS system" was made in error.

Marko Elez

Mr. Elez's access to NDNH has been deactivated.

Mr. Elez has neither installed nor requested to be installed any unapproved software on HHS networks or systems.

Aram Moghaddassi

Aram Moghaddassi is an employee of DOL and has been detailed to HHS since March 5, 2025,

in furtherance of the DOGE EO, and has no employment relationship with DOGE.

Mr. Moghaddassi has been granted permission to access the following Sensitive Systems at HHS:

1. GrantSolutions on February 19, 2025, by the Director, Security and Data Project Management Office, HHS Office of Grants;
2. National Directory of New Hires (NDNH) database on March 6, 2025, by the Administration for Children and Families (ACF) Chief Technology Officer;
3. CMS Acquisition Lifecycle Modernization (CALM) system on March 5, 2025, by the Chief Information Officer, CMS Office of Information Technology;
4. Integrated Data Repository (IDR) at CMS on March 5, 2025, by the Chief Information Officer, CMS Office of Information Technology; and
5. Healthcare Integrated General Ledger Accounting System (HIGLAS) on March 5, 2025, by the Chief Information Officer, CMS Office of Information Technology.

Mr. Moghaddassi was granted read-only access to the above-listed systems. Mr. Moghaddassi's access to NDNH has been deactivated.

Mr. Moghaddassi accessed CALM, IDR, and HIGLAS in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Mr. Moghaddassi has not modified, copied and shared with any unauthorized users, or removed any records from any of these systems. There are currently no pending requests to grant Mr. Moghaddassi access to other sensitive systems at HHS, nor has Mr. Moghaddassi been denied access to any systems at HHS.

Mr. Moghaddassi acknowledged the Rules of Behavior for General Users, the Rules of Behavior for Privileged Users, and completed Cybersecurity training.

Mr. Moghaddassi has neither installed nor requested to be installed any unapproved software on HHS networks or systems.

Conor Fennessy

Conor Fennessy is an employee of the Department of Education and has been detailed to HHS

since February 20, 2025, in furtherance of the DOGE EO, and has no employment relationship with USDS.

Mr. Fennessy has been granted permission to access the following Sensitive Systems at HHS:

1. CMS Acquisition Lifecycle Modernization (CALM) system on March 3, 2025, by the Chief Information Officer, CMS Office of Information Technology;
2. Health Resources and Services Administration's (HRSA's) Electronic Handbooks (EHBs);
3. NIH Business System EBS and PRISM systems on February 28, 2025, by the NIH Office of the Chief Information Officer;
4. Financial Business Intelligence System (FBIS) on March 7, 2025, but was not granted access to view PII data, by the office of the Assistant Secretary for Financial Resources (ASFR);
5. Grants.gov on February 28, 2025, by the office of the ASFR;
6. HHS Consolidated Acquisition System (HCAS) on February 28, 2025, by Executive Director, Strategic Programs and Business Systems at the office of the ASFR; and
7. GrantSolutions on February 28, 2025, by the Director, Security and Data Project Management Office, HHS Office of Grants.

Mr. Fennessy was granted read-only access to the above-listed systems. Mr. Fennessy's access to the CALM system, FBIS, HCAS, and NIH EBS System has been deactivated.

Mr. Fennessy accessed HCAS, HRSA's EHBs and the NIH Acquisition System in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Mr. Fennessy has not modified, copied and shared with any unauthorized users, or removed any records from any of these systems. There are currently no pending requests to grant Mr. Fennessy access to other sensitive systems at HHS, nor has Mr. Fennessy been denied access to any systems at HHS.

Mr. Fennessy acknowledged the Rules of Behavior for General Users, completed NIH Remote

Access and Security Training, and completed Cybersecurity training.

Mr. Fennessy has neither installed nor requested to be installed any unapproved software on HHS networks or systems.

Jeremy Lewin

Jeremy Lewin is an employee of GSA and has been detailed to HHS since February 21, 2025, in furtherance of the DOGE EO, and has no employment relationship with USDS.

Mr. Lewin has been granted permission to access the following Sensitive Systems at HHS:

1. GrantSolutions on February 28, 2025, by the Director, Security and Data Project Management Office, HHS Office of Grants;
2. CMS Acquisition Lifecycle Modernization (CALM) system on March 3, 2025, by the Chief Information Officer, CMS Office of Information Technology; and
3. Health Resources and Services Administration's (HRSA's) Electronic Handbooks (EHBs).

Mr. Lewin was granted read-only access to the above-listed systems. Mr. Lewin's access to the CALM system has been deactivated.

Mr. Lewin accessed HRSA's EHBs in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Mr. Lewin has not modified, copied and shared with any unauthorized users, or removed any records from any of these systems. There are currently no pending requests to grant Mr. Lewin access to other sensitive systems at HHS, nor has Mr. Lewin been denied access to any systems at HHS.

Mr. Lewin acknowledged the Rules of Behavior for General Users and completed Cybersecurity training.

Mr. Lewin has neither installed nor requested to be installed any unapproved software on HHS networks or systems.

Zach Terrell

Zach Terrell is an employee of HHS since March 6, 2025, and has no employment relationship with USDS.

Mr. Terrell has been granted permission to access the following Sensitive Systems at HHS:

1. Integrated Data Repository (IDR) at CMS on March 11, 2025, by the Chief Information Officer, CMS Office of Information Technology;
2. Health Resources and Services Administration's (HRSA's) Electronic Handbooks (EHBs);
3. Enterprise Human Capital Management (EHCM) on March 7, 2025, by the HR Information System Security Officer;
4. Payment Management System (PMS) on March 27, 2025, by the Chief Technology Officer, Program Support Center;
5. HHS Unified Financial Management System (UFMS), but only the application and not the database, on March 18, 2025, by the office of the Assistant Secretary for Financial Resources (ASFR); and
6. Financial Business Intelligence System (FBIS), but only the application and not the database and was not granted access to view PII data, on or about March 16, 2025, by the office of the ASFR.

Mr. Terrell was granted read-only access to the above-listed systems.

Mr. Terrell accessed IDR, HRSA's EHBs, and PMS in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Mr. Terrell has not modified, copied and shared with any unauthorized users, or removed any records from any of these systems. There are currently no pending requests to grant Mr. Terrell access to other sensitive systems at HHS, nor has Mr. Terrell been denied access to any systems at HHS.

Mr. Terrell acknowledged the Rules of Behavior for General Users, the Rules of Behavior for Privileged Users, and completed Cybersecurity training.

Mr. Terrell has neither installed nor requested to be installed any unapproved software on HHS networks or systems.

Rachel Riley

Rachel Riley is an employee of HHS since January 27, 2025, and has no employment relationship with USDS.

Ms. Riley has been granted permission to access the following Sensitive Systems at HHS:

1. CMS Acquisition Lifecycle Modernization (CALM) system on February 3, 2025, by the Chief Information Officer, CMS Office of Information Technology;
2. NIH Business System EBS and PRISM systems on February 24, 2025, by the NIH Office of the Chief Information Officer;
3. Enterprise Human Capital Management (EHCM) on February 3, 2025, by the Office of the Chief Information Officer;
4. Financial Business Intelligence System (FBIS) on February 4, 2025, but was not granted access to view PII data, by the office of the Assistant Secretary for Financial Resources;
5. GrantSolutions on February 20, 2025, by the Director, Security and Data Project Management Office, HHS Office of Grants;
6. HHS Consolidated Acquisition System (HCAS) on February 3, 2025, by Executive Director, Strategic Programs and Business Systems at ASFR; and
7. Business Intelligence Information System on February 6, 2025, by the Office of the Chief Information Officer.

Ms. Riley was granted administrator privileges for HCAS, and read-only access to the other systems listed above. Ms. Riley's access to HCAS has been deactivated.

Ms. Riley accessed HCAS, CALM, EHCM, and FBIS in furtherance of the DOGE EO's directive to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. Ms. Riley has not modified, copied and shared with any unauthorized users, or removed any records from any HHS systems. There are currently no pending requests to grant Ms.

Riley access to other sensitive systems at HHS, nor has Ms. Riley been denied access to any systems at HHS.

As part of her onboarding process at HHS, Ms. Riley acknowledged the Rules of Behavior for General Users and completed Cybersecurity training. Ms. Riley also completed the NIH Information Security and Information Management Training; the 2024 Information Security and Management Refresher; Remote Access and Security Training; and acknowledged the NIH Access/Disclosure Agreement for the Office of Human Resources.

Ms. Riley has neither installed nor requested to be installed any unapproved software on HHS networks or systems.

Brad Smith

Brad Smith is an HHS employee as of March 4, 2025, and is also an employee of DOGE. Mr. Smith has not been granted permission to access any HHS Sensitive Systems.

B. Revised Response as to the U.S. Department of Labor

Marko Elez

Mr. Elez is the only DOL employee who has an employment relationship with USDS and who has been granted permission to access sensitive systems at the agency.

Mr. Elez has been granted permission to access four sensitive systems: (i) USAccess on February 25, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management; (ii) DOL Homeland Security Presidential Directive 12 (HSPD-12) Enterprise Physical Access Control System (EPACS) on February 25, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management; (iii) DOL Directory Resource Administrator (DRA) on February 25, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management; and (iv) Unemployment Insurance Data and Related Records on March 21, 2025, by Thomas Shedd, Chief Information Officer.

Mr. Elez was granted access to the above-listed systems in furtherance of the directive in Executive Order 14,158 (the USDS EO) to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. To gain access to the systems, Mr. Elez signed Rules of Behavior for each system. As of March 26, 2025, Mr. Elez has not accessed any of the systems.

Mr. Elez has installed, or caused to be installed, two programs on DOL systems, Visual Studio Code, a code editor, and Python, a programming language.

Mr. Elez has been denied access to two systems: (i) ASAP.gov and (ii) Adobe Licensing Portal.

DOL is aware of four other agencies at which Mr. Elez is concurrently detailed to or otherwise employed, other than USDS. **Aram Moghaddassi**

Mr. Moghaddassi does not have an employment relationship with USDS, but is a member of DOL's DOGE Team. Mr. Moghaddassi is an employee of the Department of Labor.

Mr. Moghaddassi has been granted permission to access five sensitive systems: (i) USAccess on February 26, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management; (ii) DOL Homeland Security Presidential Directive 12 (HSPD-12) Enterprise Physical Access Control System (EPACS) on February 26, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management; (iii) HR Connect on February 19, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management; (iv) New Core Financial Management System (NCFMS) on February 20, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management, (v) Unemployment Insurance Data and Related Records on March 21, 2025, by Thomas Shedd, Chief Information Officer.

Mr. Moghaddassi was granted access to the above-listed systems in furtherance of the directive in Executive Order 14,158 (the USDS EO) to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. In order to gain access to the systems, Mr. Moghaddassi signed Rules of Behavior for each system. DOL believes that Mr. Moghaddassi has accessed all these systems.

As of April 3, 2025, Mr. Moghaddassi has not installed or caused to be installed any software on DOL systems.

Mr. Moghaddassi has been denied access to two systems: (i) ASAP.gov and (ii) Adobe Licensing Portal.

DOL is aware of four other agencies at which Mr. Moghaddassi is concurrently detailed to or otherwise employed.

Miles Collins

Mr. Collins does not have an employment relationship with USDS, but is a member of DOL's DOGE Team. Mr. Collins is an employee of the Department of Labor.

Mr. Collins has been granted permission to access five sensitive systems: (i) Payment Management System (PMS), an HHS shared service system used by DOL to process grant payments. DOL believes that HHS granted access to the system, (ii) Office of Job Corps Electronic Information System (OJC EIS) on March 20, 2025, by Dean Heyl, Assistant Secretary for Administration and Management; (iii) HR Connect on February 19, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management; (iv) DOL Directory Resource Administrator (DRA) on February 26, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management, and (v) New Core Financial Management System (NCFMS) on

February 20, 2025, by Troy Finnegan, Former Assistant Secretary for Administration and Management.

Mr. Collins was granted access to the above-listed systems in furtherance of the directive in Executive Order 14,158 (the USDS EO) to identify waste, fraud, and abuse and to modernize government technology and software to increase efficiency and productivity. In order to gain access to the systems, Mr. Collins signed Rules of Behavior for DRA, HR Connect and NCFMS. For OJC EIS Rules of Behavior are completed as part of the initial login. DOL is unaware of whether Rules of Behavior were signed for PMS. As of April 3, 2025, Mr. Collins has accessed PMS, OJC EIS, and is not sure whether he has accessed HR Connect. Mr. Collins has not accessed DRA and NCFMS.

Mr. Collins has been denied access to two systems: (i) ASAP.gov and (ii) Adobe Licensing Portal.

DOL is not aware of any other agencies at which Mr. Collins is concurrently detailed to or otherwise employed.

C. Revised Response as to the Consumer Financial Protection Bureau

Jordan Wick: Mr. Wick is a CFPB employee and an employee of USDS. He was onboarded as a CFPB employee on March 5 (while remaining an employee of USDS). Prior to that, he was detailed to the CFPB from USDS.

Christopher Young: Mr. Young is detailed from the Office of Personnel Management to CFPB. Mr. Young is also detailed to USDS.

Gavin Kliger: Mr. Kliger is detailed from the Office of Personnel Management to CFPB.

Jeremy Lewin: Mr. Lewin is detailed from the General Services Administration to CFPB.

Nikhil Rajpal: Mr. Rajpal was detailed from the Office of Personnel Management to CFPB until March 21, 2025. Mr. Rajpal was also detailed to USDS.

Luke Farritor: Mr. Farritor was detailed from the Government Services Administration to CFPB until March 4, 2025. Mr. Farritor was also detailed to USDS.

As to part a:

Jordan Wick: Mr. Wick was granted access to the following Sensitive Systems: Entra ID, Procurement Request Information System Management (PRISM), HRConnect, webTA, Data Insight, USAStaffing, Invoice Processing Platform (IPP), Oracle Business Intelligence (OBI), oneARC, G-Invoicing, and Concur. Mr. Wick was also authorized to access, but was not ultimately granted access, to Active Directory and Physical Access Control.

Christopher Young: Mr. Young was not granted access to any Sensitive Systems.

Gavin Kliger: Mr. Kliger was granted access to Active Directory, Entra ID, and Physical Access Control.

Jeremy Lewin: Mr. Lewin was not granted access to any Sensitive Systems.

Nikhil Rajpal: Mr. Rajpal was authorized to access, but was not ultimately granted access to, Active Directory, Entra ID, and Physical Access Control.

Luke Farritor: Mr. Farritor was granted access to Active Directory and Entra ID. Mr. Farritor was also authorized to access but was not ultimately granted access to Physical Access Control.

As to part b:

Jordan Wick: Mr. Wick was granted permission to access the Sensitive Systems listed above on February 7, except for Entra ID, the permission for which was granted on February 9.

Gavin Kliger: Mr. Kliger was granted permission to access the Sensitive Systems listed above on February 7.

Nikhil Rajpal: Mr. Rajpal was granted permission to access the Sensitive Systems listed

above on February 7.

Luke Farritor: Mr. Farritor was granted permission to access the Sensitive Systems listed above on February 7.

As to part c:

Chris Chilbert, Chief Information Officer, authorized Mr. Wick's, Mr. Klinger's, Mr. Rajpal's, and Mr. Farritor's access to Active Directory, Entra ID, and Physical Access Control. In addition, the following CFPB staff authorized Mr. Wick's access to the other Sensitive Systems referenced above: Joshua Galicki of the Office of Finance and Procurement approved access to PRISM; Nikki L. DiPalma of the Office of Human Capital approved access to HRConnect, webTA, Data Insight, and USAStaffing; Antona Bailey of the Office of Finance and Procurement approved access to the IPP, OBI, and oneARC systems; Sheryl Kidd of the Office of Finance and Procurement approved access to G-Invoicing; and Regina Braham of the Office of Finance and Procurement approved access to Concur.

As to part d:

All six individuals listed above completed Privacy training, which was administered by the CFPB's Chief Privacy Officer on February 7, 2025, using the PowerPoint produced in response to document request 5. Mr. Wick, Mr. Young, Mr. Kliger, and Mr. Rajpal also completed the Bureau's Cybersecurity Awareness Training within 30 days of onboarding, as set forth in Bureau policy. Mr. Farritor completed his detail before his Cybersecurity Awareness Training was required to be completed, as detailed in the document titled Cybersecurity Training Overview. Mr. Lewin did not complete Cybersecurity Awareness Training.

Mr. Wick, Mr. Young, Mr. Kliger, Mr. Lewin, and Mr. Farritor also certified in their respective Detailee Certifications of Compliance that their access to CFPB systems would be

conducted in compliance with all relevant federal security, ethics, and confidentiality laws, regulations, and policies, including CFPB records management and information security requirements.

Additionally, the MOU agreement for Mr. Rajpal's detail assignment provided that he would not knowingly access CFPB systems in a manner that fails to comply with all relevant federal, security, ethics, and confidentiality laws, regulations, and policies, including the CFPB records management and information security requirements.

As to part e:

Jordan Wick: Mr. Wick accessed Entra ID, which operates to govern access for users in the Microsoft environment, to assess the system's capabilities and the level of access granted. In addition, pursuant to a direction from a CFPB official to Mr. Wick to send an email with specified contents using that official's email address, Mr. Wick used the EntraID system to authorize himself to send that email using that official's email address. There were no restrictions on Mr. Wick's access to Entra ID until March 5, at which point access was removed.

Mr. Wick used PRISM, the CFPB's procurement system for managing contracts, to review the CFPB's contracts. He had read-only access and thus could not modify or terminate any contracts in that system. On March 28, 2025, Mr. Wick's access to PRISM was removed pursuant to a court order in *American Federation of Teachers et al. v Bessent et al.*, No. 8:25-cv-430 (D. Md. Mar. 28, 2025).

Mr. Wick had read-only access to IPP, OBI, and oneARC systems, which contain information regarding the CFPB's finances. He used these systems to assess the systems' capabilities and the level of access granted. He did not have the ability to change the underlying data in any of these systems. Mr. Wick had the ability to run reports in OBI, and did so to review

information on existing contracts. On March 28, 2025, Mr. Wick's access to IPP, OBI, and oneARC was removed pursuant to the court order noted above.

Mr. Wick had read-write-delete access to HRConnect, the CFPB's primary human resource system. With support from a CFPB HR official, Mr. Wick used this access to assess the system's capabilities and learn its functions. He did not alter any records. Mr. Wick used Data Insight, which is a read-only reporting system, to review the names of CFPB employees and the divisions in which they work. Mr. Wick had view-only access to USA Staffing, which allowed him to see information related to vacancies and new hires. Mr. Wick used this system to access whether any CFPB staff were hired after the imposition of the federal hiring freeze. On March 28, 2025, Mr. Wick's access to HRConnect, Data Insight, and USA Staffing was removed pursuant to the court order noted above.

While authorized, Mr. Wick was not granted access to the Physical Access Control system. Nor does the CFPB have any record that Mr. Wick ever accessed G-Invoicing, webTA, or Concur. On March 28, 2025, Mr. Wick's access to G-Invoicing, webTA, and Concur was removed pursuant to the court order noted above. Mr. Wick did not copy, share, or remove information outside of these systems.

Finally, until March 5, Mr. Wick had sufficient permission rights to grant himself and others access to systems containing both market monitoring information and supervision, enforcement and fair lending data. Mr. Wick did not, however, grant himself or others such access.

Christopher Young: Mr. Young was not granted access to any Sensitive Systems.

Gavin Kliger: Mr. Kliger logged into Physical Access Control once, to confirm his access and to receive a tutorial on the system. Mr. Kliger did not ultimately use that system. And while granted access, Mr. Kliger never ultimately accessed Active Directory or Entra ID. Finally, until

February 8, Mr. Kliger had sufficient permission rights to grant himself and others access to systems containing both market monitoring information and supervision, enforcement and fair lending data. Mr. Kliger did not, however, grant himself or others such access. Mr. Kliger did not have access to any other Sensitive Systems. Mr. Kliger did not copy, share, or remove information outside these systems.

Jeremy Lewin: Mr. Lewin was not granted access to any Sensitive Systems.

Nikhil Rajpal: While authorized, Mr. Rajpal was not ultimately granted access to any Sensitive Systems.

Luke Farritor: Mr. Farritor used Entra ID to provide access to Gavin Kliger to the systems necessary to update the CFPB's public-facing website. Mr. Farritor logged into Active Directory to confirm his access but did not ultimately use that system. Mr. Farritor did not copy, share, or remove information outside these systems. Mr. Farritor did not have access to any other Sensitive Systems. Prior to his departure, Mr. Farritor had sufficient permission rights to grant himself and others access to systems containing both market monitoring information and supervision, enforcement and fair lending data. Mr. Farritor did not, however, grant himself or others such access.

As to part f:

The six individuals described in this response were not granted the permission to install or cause to be installed any software on the CFPB's networks or systems. The CFPB is not aware of any evidence that these individuals installed or caused to be installed any software on the CFPB's networks or systems.

As to part g:

CFPB officials approved access to each system requested by Mr. Wick over which CFPB

officials had authority to approve access to. There were several systems, however, that Mr. Wick requested access to that are maintained by the Department of Treasury's Bureau of Fiscal Services and that the CFPB does not utilize. Access to those system—specifically, OneStream and Oracle—was denied.

As to part h:

The CFPB does not maintain information on DOGE Employees' concurrent details. On information and belief, Mr. Rajpal has been detailed to two federal agencies besides the CFPB and USDS; Mr. Farritor has been detailed to at least four federal agencies besides the CFPB and USDS; Jordan Wick is an employee at one other agency and detailed to at least six agencies besides CFPB and USDS; Mr. Kliger has been detailed to nine federal agencies besides the CFPB; and Mr. Lewin has been detailed to four federal agencies besides his home agency and the CFPB.

INTERROGATORY NO. 2: With respect to structure of DOGE and the relationship between DOGE and DOGE Employees detailed to Defendant Agencies,

- i. Identify the individual who has been appointed to or is, in fact, serving in the role of the USDS Administrator, as that term is used in Section 3(b) of Executive Order 14158.
- j. Identify any individual(s) within DOGE or the Executive Office of the President who exercises authority over government-wide DOGE operations, including with respect to the following decisions:
 - i. Which agencies a DOGE Employee will be detailed or otherwise deployed to;
 - ii. Which DOGE Employees to deploy to each agency;

- iii. How a DOGE Employee should implement the President's "DOGE Agenda" at agencies, including the scope of work to be performed at agencies; and
- iv. How a DOGE Employee should resolve conflicts with employees of Defendant Agencies concerning the scope of the authority DOGE Employees may exercise at the agencies or the scope of the DOGE Employee's access to the Sensitive Systems of one of the Defendant Agencies.
- k. If there are multiple individuals within the Executive Office of the President who exercise authority related to the detailing or deployment of DOGE Employees to Defendant Agencies, please (i) identify all such individuals and (ii) describe the scope of their authority.
- l. Identify the circumstances under which information gathered from Sensitive Systems may be shared between a DOGE Employee detailed or otherwise deployed to one of the Defendant Agencies and any persons not employed by Defendant Agencies, such as DOGE Employees detailed to or otherwise employed by different agencies (even if the different agency is also one of the Defendant Agencies), DOGE Employees not detailed to or otherwise employed by any agency, employees at other federal agencies or within the White House Executive Office of the President, or individuals who are not government employees;
- m. Identify the individual(s) within the federal government who have the authority to supervise, discipline, terminate, or reinstate a DOGE Employee who has been detailed to or is otherwise employed by one of the Defendant Agencies.

Objections: Defendants object that these requests are not relevant to Plaintiffs’ forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.’ Mot. for Reconsideration, ECF No. 51. Defendants further object that these requests are premature, as set forth in General Objection 2. Defendants further object to this request to the extent it calls for privileged information, as set forth in General Objection 4. Defendants further object to the term “DOGE Employee,” as set forth in General Objection 5. Defendants further object to the term “Sensitive Systems,” as set forth in General Objection 6.

Defendants further object to the extent Plaintiffs seek information about individuals who are no longer detailed to, or employed at, one of the Agency Defendants. Defendants further object to subpart j on the grounds that it seeks evidence about USDS’s practices at agencies other than CFPB, HHS, and DOL, which is not relevant to Plaintiffs’ forthcoming preliminary injunction motion and would impose burdens disproportionate to the needs of the case. Defendants further object that the phrase “exercises authority” in subpart j and subpart k, and the term “authority” in subpart m, are vague and ambiguous. Defendants recognize Plaintiffs’ email of April 1, 2025, redefining “authority” to mean “actual authority.” Defendants believe this definition is still vague and ambiguous. Defendants will interpret this newly defined term to encompass two concepts: “formal legal authority” and “authority” defined to mean the “[p]ower or right to give orders, make decisions, and enforce obedience.” *Authority*, Oxford English Dictionary, https://www.oed.com/dictionary/authority_n?tab=meaning_and_use#33130898. Defendants further object to part l on the basis that it calls for a legal conclusion as to “the circumstances under which information gathered from Sensitive Systems may be shared between a DOGE Employee detailed to one of the Defendant Agencies and any persons not employed by Defendant Agencies,”

which are determined by statutes such as the Privacy Act. Defendants further object to subparts j and k because USDS, and not the Executive Office of the President more broadly, is the only named defendant in this action. Defendants further object to subpart l because it requires Defendants to speculate about unspecified “circumstances under which information gathered from Sensitive Systems may be shared” with government employees, which depends upon the type of information being shared, the system from which the information was taken, the identity of the person or entity with whom the information is being shared, and the purpose for which the information is shared. As such, the request is overly broad, unduly burdensome, and disproportionate to the needs of the case.

A. Response from USDS

As to part i, Amy Gleason is Acting Administrator of USDS.

As to part j, in her capacity as Acting Administrator of USDS, Ms. Gleason exercises authority over detailing and deploying DOGE Employees from USDS to other agencies. This includes executing detail agreements between USDS and other agencies. Whether an agency chooses to onboard a USDS employee, or accept a detail, is up to that agency.

Defendant Agency leadership determines how to implement the President’s “DOGE Agenda” at each respective agency. This includes determining the scope of DOGE Employees’ access to Sensitive Systems and their authority at each agency.

As to part k, see the response to Interrogatory 2(b), above.

As to part l, information from Sensitive Systems may be shared to the extent needed to facilitate the DOGE Agenda as implemented by the relevant agency and consistent with applicable law, which may include, among other things, the Privacy Act, agency System of Records Notices, and agency-specific restrictions.

As to part m, there are no USDS Employees detailed to Defendant Agencies. Defendant Agency leadership is responsible for supervising, terminating, etc. a DOGE employee employed by the relevant Defendant Agency in their capacity as an agency employee.

IV. SPECIFIC OBJECTIONS AND RESPONSES TO REQUESTS FOR PRODUCTION

Request for Production 1: Copies of any nondisclosure agreements signed by DOGE Employees detailed to or otherwise employed by Defendant Agencies, including but not limited to the nondisclosure agreements referenced in the Declaration of Adam Martinez, ECF No. 31-3 ¶ 6 and any similar agreements that may exist at other Defendant Agencies.

Objections: Defendants object that these requests are not relevant to Plaintiffs' forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.' Mot. for Reconsideration, ECF No. 51. Defendants further object that these requests are premature, as set forth in General Objection 2. Defendants object to the term "DOGE Employee," as set forth in General Objection 5. Defendants further object to the terms "nondisclosure agreements" and "similar agreements" as they are undefined and vague, as the parties may have different understandings of what constitutes such agreements.

Response: Subject to these objections, Defendants will, within the parameters of the limited time frame for discovery the Court ordered, perform a reasonable and proportional search for documents responsive to this request and produce responsive, non-privileged documents. Defendants reserve the right to redact sensitive personally identifiable information from these documents.

Request for Production 2: Copies of any written agreements or certifications governing or describing the detail of DOGE Employees to Defendant Agencies (or employment by DOGE

Employees by Defendant Agencies), including but not limited to the detail agreements referenced in the Declaration of Garey Rice, ECF No. 31-2 ¶ 7, the Martinez Decl., ECF No. 31-3 ¶ 8, the memorandum of understanding that is in place between HHS and another federal agency, which is referenced in the Rice Decl., ECF No. 31-2 ¶ 8, task orders describing DOGE’s responsibilities in the declaration of Ricky J. Kryger, ECF No. 31-1 ¶ 5, detail agreements effectuating the DOGE detail described in the Declaration of Adam Ramada, ECF No. 16-1 ¶ 6, and any other similar agreements setting forth or describing the terms of DOGE’s work at Defendant Agencies.

Objections: Defendants object that these requests are not relevant to Plaintiffs’ forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.’ Mot. for Reconsideration, ECF No. 51. Defendants further object that these requests are premature, as set forth in General Objection 2. Defendants further object to the term “DOGE Employee,” as set forth in General Objection 5. Defendants further object to the terms “task orders” and “similar agreements” as they are undefined and vague, as the parties may have different understandings of what constitutes such agreements.

Response: Subject to these objections, Defendants will, within the parameters of the limited time frame for discovery the Court ordered, perform a reasonable and proportional search for documents responsive to this request and produce responsive, non-privileged documents. Defendants reserve the right to redact sensitive personally identifiable information from these documents

Request for Production 3: Copies of any written guidelines for DOGE Employees’ access to Sensitive Systems, including but not limited to the guidelines referred to in the Kryger declaration, ECF No. 31-1 ¶ 8, and any other similar guidelines that may exist at Defendant Agencies.

Objections: Defendants object that these requests are not relevant to Plaintiffs' forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.' Mot. for Reconsideration, ECF No. 51. Defendants further object that these requests are premature, as set forth in General Objection 2. Defendants further object to the term "DOGE Employee," as set forth in General Objection 5. Defendants further object to the term "Sensitive Systems," as set forth in General Objection 6. Defendants further object to the term "guideline" as it is undefined and vague, as the parties may have different understandings of what constitutes guidelines.

Response: Subject to these objections, Defendants will, within the parameters of the limited time frame for discovery the Court ordered, perform a reasonable and proportional search for documents responsive to this request and produce responsive, non-privileged documents. Defendants reserve the right to redact sensitive personally identifiable information from these documents.

Request for Production 4: Copies of any certifications or access agreements signed by DOGE Employees or their supervisors in order to grant them access to Sensitive Systems, including but not limited to the access agreements and Request to Access forms referenced to in the Kryger declaration, ECF No. 31-1 ¶ 8, any written authorization referenced to in the Martinez Decl., ECF No. 31-3 ¶ 9, and any other similar authorizations that may exist at Defendant Agencies.

Objections: Defendants object that these requests are not relevant to Plaintiffs' forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.' Mot. for Reconsideration, ECF No. 51. Defendants further object that these requests are premature, as set forth in General Objection 2.

Defendants further object to the term “DOGE Employee,” as set forth in General Objection 5. Defendants further object to the term “Sensitive Systems,” as set forth in General Objection 6. Defendants further object to the terms “certifications,” “access agreements,” and “similar authorizations” as it is undefined and vague, as they are undefined and vague, as the parties may have different understandings of what constitutes such agreements.

Response: Subject to these objections, Defendants will, within the parameters of the limited time frame for discovery the Court ordered, perform a reasonable and proportional search for documents responsive to this request and produce responsive, non-privileged documents. Defendants reserve the right to redact sensitive personally identifiable information from these documents.

Request for Production 5: Copies of any privacy and/or cyber security training materials or documents provided to DOGE Employees on detail to Defendant Agencies, as referenced in in [sic] the Martinez Decl., ECF No. 31-3 ¶ 6.

Objections: Defendants object that these requests are not relevant to Plaintiffs’ forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.’ Mot. for Reconsideration, ECF No. 51. Defendants further object that these requests are premature, as set forth in General Objection 2. Defendants further object to the term “DOGE Employee,” as set forth in General Objection 5. Defendants further object to the extent that some trainings are only offered through online modules, and within the time constraints of the Court’s order directing expedited discovery, extracting such online modules into a producible format is overly burdensome and disproportionate to the needs of Plaintiffs’ forthcoming motion for a preliminary injunction.

Response: Subject to these objections, Defendants will, within the parameters of the limited time frame for discovery the Court ordered, perform a reasonable and proportional search for documents responsive to this request and produce responsive, non-privileged documents. Defendants reserve the right to redact sensitive personally identifiable information from these documents.

Request for Production 6: Copies of any “confidentiality protocols” established to govern the access of DOGE Employees, as referenced in the Kryger declaration, ECF No. 31-1 ¶ 9, and any other similar authorizations that exist at the Defendant Agencies.

Objections: Defendants object that these requests are not relevant to Plaintiffs’ forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.’ Mot. for Reconsideration, ECF No. 51. Defendants further object that these requests are premature, as set forth in General Objection 2. Defendants further object to the term “DOGE Employee,” as set forth in General Objection 5. Defendants object to the term “confidentiality protocols,” to the extent it includes documents outside those outlined in the Kryger declaration, as vague, as the parties may have different understandings of what constitutes such agreements.

Response: Subject to these objections, Defendants will, within the parameters of the limited time frame for discovery the Court ordered, perform a reasonable and proportional search for documents responsive to this request and produce responsive, non-privileged documents. Defendants reserve the right to redact sensitive personally identifiable information from these documents.

Request for Production 7: Copies of any documents or records in which the DOL Office of the Chief Information Officer (“OCIO”) granted “specific approval” for users of “the data,

information, or documents from DOL information systems . . . to share this data, information, or documents outside of DOL information systems,” as referenced in the Kryger declaration, ECF No. 31-1 ¶ 11, and any similar approvals granted at other Defendant Agencies. This request is limited to approvals for the sharing of data, information, or records by or to a DOGE Employee.

Objections: Defendants object that these requests are not relevant to Plaintiffs’ forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.’ Mot. for Reconsideration, ECF No. 51. Defendants further object that these requests are premature, as set forth in General Objection 2. Defendants further object to the term “DOGE Employee,” as set forth in General Objection 5. Defendants object to the term “similar approvals” as vague, as the parties may have different understandings of what constitutes such approvals.

Response: Subject to these objections, Defendants will, within the parameters of the limited time frame for discovery the Court ordered, perform a reasonable and proportional search for documents responsive to this request and produce responsive, non-privileged documents. Defendants reserve the right to redact sensitive personally identifiable information from these documents.

IV. SPECIFIC OBJECTIONS DEPOSITION NOTICES

Objections to the Notices to the Defendant Agencies: Defendants object that the noticed 30(b)(6) depositions are not relevant to Plaintiffs’ forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.’ Mot. for Reconsideration, ECF No. 51. Defendants object that these notices are premature, as set forth in General Objection 2. Defendants further object to the deposition notices to the extent they call for testimony about privileged information, as set forth in General Objection 4. Defendants further object to the term “DOGE Employee,” as set forth in General Objection 5.

Defendants further object to the term “Sensitive Systems,” as set forth in General Objection 6. Defendants further object to the terms “Access” and “Accessed,” as set forth in General Objection 7. Defendants further object to the terms “record” and “records,” as set forth in General Objection 8. Defendants further object to the extent Plaintiffs seek information about individuals who are no longer detailed to, or employed at, one of the Agency Defendants. Defendants further object that the term “authority” in the second topic is vague and ambiguous. Defendants recognize Plaintiffs’ email of April 1, 2025, redefining “authority” to mean “actual authority.” Defendants believe this definition is still vague and ambiguous. Defendants will interpret this newly defined term to encompass two concepts: “formal legal authority” and “authority” defined to mean the “[p]ower or right to give orders, make decisions, and enforce obedience.” *Authority*, Oxford English Dictionary, https://www.oed.com/dictionary/authority_n?tab=meaning_and_use#33130898. Defendants further object to topic 3 on the grounds that “actual usage” is vague and ambiguous, and that preparing witnesses on the usage of each Sensitive System by any DOGE Employee, as described therein, is overbroad, unduly burdensome, and disproportionate to the needs of the case.

Objections to Notice to USDS: Defendants object that the noticed 30(b)(6) depositions are not relevant to Plaintiffs’ forthcoming motion for a preliminary injunction because Defendants are no longer detailing USDS employees to work at the Defendant Agencies. *See* Defs.’ Mot. for Reconsideration, ECF No. 51. Defendants object that these notices are premature, as set forth in General Objection 2. Defendants further object to the deposition notices to the extent they call for testimony about privileged information, as set forth in General Objection 4. Defendants further object to the term “DOGE Employee,” as set forth in General Objection 5. Defendants further object to the term “Sensitive Systems,” as set forth in General Objection 6. Defendants further object to the terms “Access” and “Accessed,” as set forth in General Objection 7. Defendants

further object to the terms “record” and “records,” as set forth in General Objection 8. Defendants further object to the extent Plaintiffs seek information about individuals who are no longer detailed to, or employed at, one of the Agency Defendants. Defendants further object that the term “authority” in the second and third topics is vague and ambiguous. Defendants recognize Plaintiffs’ email of April 1, 2025, redefining “authority” to mean “actual authority.” Defendants believe this definition is still vague and ambiguous. Defendants will interpret this newly defined term to encompass two concepts: “formal legal authority” and “authority” defined to mean the “[p]ower or right to give orders, make decisions, and enforce obedience.” *Authority*, Oxford English Dictionary, https://www.oed.com/dictionary/authority_n?tab=meaning_and_use#331308

98. Defendants further object to topic 3 on the grounds that “use” is vague and ambiguous, and that preparing a witness on the use of each Sensitive System by any DOGE Employee, as described therein, is overbroad, unduly burdensome, and disproportionate to the needs of the case.

* * *

As to the interrogatory responses, see the attached verifications.

As to the objections and the responses to the requests for production,

Dated: April 4, 2025

Respectfully submitted,

YAAKOV M. ROTH
Acting Assistant Attorney General
Civil Division

MARCIA BERMAN
Assistant Branch Director
Civil Division, Federal Programs Branch

/s/ Bradley P. Humphreys
Bradley P. Humphreys (D.C. Bar No. 988057)
Senior Trial Counsel
Andrew M. Bernie (D.C. Bar No. 995376)

Trial Attorney
Benjamin S. Kurland (D.C. Bar No. 1617521)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, NW
Washington, DC 20005
Telephone: (202) 305-0878
Bradley.Humphreys@usdoj.gov

CERTIFICATE OF SERVICE

I certify that I served a true and correct copy of Defendants' Objections and Responses to Plaintiffs' Requests for Expedited Discovery on counsel of record in this case via e-mail on April 4, 2025.

/s/ Bradley P. Humphreys
Bradley P. Humphreys

VERIFICATION OF INTERROGATORY ANSWERS

I, Christopher Chilbert, am a Chief Information Office for the Consumer Financial Protection Bureau (CFPB). I believe, based on a reasonable inquiry, that the foregoing answers to interrogatories on behalf of CFPB are true and correct to the best of my knowledge, information, and belief.

I verify under penalty of perjury that the foregoing is true and correct.

Executed on April 4, 2025

CHRISTOPHER
CHILBERT

Digitally signed by CHRISTOPHER
CHILBERT
Date: 2025.04.04 09:37:07 -04'00'

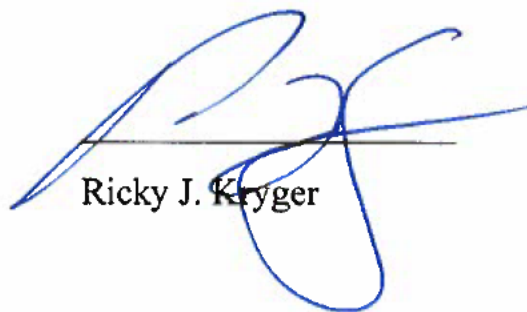
Christopher Chilbert

VERIFICATION OF INTERROGATORY ANSWERS

I, Ricky J. Kryger, am Deputy Chief Information Officer (Deputy CIO) for the Office of the Chief Information Officer (OCIO) for the United States Department of Labor (DOL) located in Washington, DC. I believe, based on a reasonable inquiry, that the foregoing answers to interrogatories on behalf of the Department of Labor, are true and correct to the best of my knowledge, information, and belief.

I verify under penalty of perjury that the foregoing is true and correct.

Executed on April 4, 2025



Ricky J. Kryger


VERIFICATION OF INTERROGATORY ANSWER

I, Clark D. Minor, am the Chief Technology Officer at the United States Department of Health & Human Services (HHS). I believe, based on a reasonable inquiry, that the foregoing answer to Interrogatory No. 1 on behalf of HHS is true and correct to the best of my knowledge, information, and belief.

I verify under penalty of perjury that the foregoing is true and correct.

Executed on April 4, 2025

**CLARK D.
MINOR -S**

 Digitally signed by CLARK
D. MINOR -S
Date: 2025.04.04 11:44:37
-04'00'

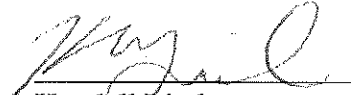
Clark D. Minor
Chief Technology Officer
U.S. Dept. of Health & Human Services

VERIFICATION OF INTERROGATORY ANSWERS

I, Kendall Lindemann, am a Senior Advisor at the United States DOGE Service (USDS), located in Washington, D.C. I believe, based on a reasonable inquiry, that the forgoing answers to interrogatories on behalf of USDS and the USDS temporary organization are true and accurate to the best of my knowledge, information, and belief.

I verify under penalty of perjury that the foregoing is true and correct.

Executed on April 4, 2025


Kendall Lindemann