U.S. Department of Justice

United States Attorney
Southern District of New York

86 Chambers Street
New York, New York 10007

July 18, 2025

By ECF
The Honorable Denise L. Cote
United States District Judge
United States Courthouse
500 Pearl St.
New York, NY 10007

Re: *Am. Fed'n of Gov't Emps., AFL-CIO, et al. v. U.S. Office of Personnel Mgmt., et al., No.* 25 Civ. 1237 (DLC)

Dear Judge Cote:

This Office represents Defendants in the above-referenced case. Pursuant to the Court's preliminary injunction order dated June 20, 2025 (ECF No. 134 at 2), we write respectfully to provide the Court with a report on behalf of the U.S. Office of Personnel Management ("OPM") which describes the processes and procedures put in place by OPM since March 6, 2025, to ensure adherence to the requirements of the Privacy Act with respect to any new grant of access permission by OPM to any records containing personally identifiable information ("PII") of the plaintiffs that exist in any OPM system of records.

Additional Processes and Procedures Implemented by OPM

OPM had established processes and procedures that were in place prior to March 6, 2025, to ensure adherence to the requirements of the Privacy Act—including appointment, training, vetting, and other data protection and privacy policies and procedures. OPM maintains that those processes and procedures are adequate to ensure compliance with the Privacy Act,[1] and OPM continues to utilize these established processes and procedures for new grants of access made to all of its employees and contractors with respect OPM systems of records.

[1] As Defendants previously noted (ECF No. 131 at 4), OPM's independent Office of the Inspector General ("OPM OIG") already conducts an annual evaluation and audit of OPM's information technology security program and practices—including data protection and privacy—to ensure compliance with the Federal Information Security Management Act. *See, e.g.,* OPM OIG, *Final Audit Report: Federal Information Security Modernization Act Audit – Fiscal Year 2023* (Oct. 30, 2024), *available at* https://www.oversight.gov/sites/default/files/documents/reports/2024-11/2024-ISAG-008.pdf. OPM OIG's 2024 annual report noted that those policies and procedures have been "consistently implemented" by OPM. *See id.* at 18-23.

Nevertheless, since April 2025, in response to a preliminary injunction issued by the District Court of the District of Maryland, OPM has documented in memoranda prepared by the Chief Information Officer, and reviewed by agency counsel, the applicable Privacy Act provision(s) which allow for access to PII in a specified OPM data system for individuals who will be granted access in connection with high profile initiatives, which include projects that could be construed as falling under the "DOGE agenda."[2]

In addition, in response to this court's preliminary injunction opinion and order (ECF Nos. 121 and 134), OPM has put in place, on an interim basis, certain additional protocols that are to be followed before granting new access to PII contained in OPM data systems to (1) any U.S. Digital Service ("DOGE") employee, contractor, or detailee, or (2) any OPM employee, contractor, or detailee hired after January 20, 2025, and who requires access for the primary purpose of working on an initiative or project involving DOGE. A copy of those interim protocols is attached to this letter as an appendix, and they have been disseminated to the appropriate staff in the Office of the Chief Information Officer, the Chief Information Security Officer, the Office of the Chief Human Capital Officer, and Facilities, Security and Emergency Management at OPM.

OPM notes that these additional measures, including the interim protocols, are not required to be implemented, including under the Privacy Act, Federal Information Security Management Act, or otherwise. In addition, these protocols pertain exclusively to internal agency management or personnel, and are not intended to, and do not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. Furthermore, these measures have been instituted as time-limited remedial measures specifically in response to the above-referenced litigations. Finally, OPM will review whether these interim protocols should remain in place 90 days after submission of this report.

Respectfully submitted,

JAY CLAYTON
United States Attorney for the
Southern District of New York

By: /s/ *David Farber*
JEFFREY OESTERICHER
DAVID E. FARBER
Assistant United States Attorneys
86 Chambers Street, Third Floor
New York, New York 10007
Tel.: (212) 637-2695/2772

cc: Plaintiffs' counsel (by ECF)

[2] The preliminary injunction in that matter was stayed pending appeal on April 7, 2025, *see Am. Fed'n of Tchrs. v. Bessent*, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025); however, OPM has still continued to prepare such memoranda since that date.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

MEMORANDUM TO: DANIELLE ROWELL
CHIEF INFORMATION SECURITY OFFICER

CARMEN GARCIA
OFFICE OF THE CHIEF HUMAN CAPITAL OFFICER

CHRISTOPHER BECKMAN
FACILITIES, SECURITY & EMERGENCY MANAGEMENT

FROM: GREG HOGAN
CHIEF INFORMATION OFFICER

BECKY RONAYNE
ACTING SENIOR AGENCY OFFICIAL FOR PRIVACY

DATE: July 18, 2025

SUBJECT: Interim Protocols for Authorizing Access to OPM Data Containing Personally Identifying Information

This memorandum is to inform you and your staff of the protocols outlined below concerning the authorization of access to OPM data systems containing personally identifying information (PII) to certain employees and contractors. These procedures are supplemental to OPM's established processes and procedures concerning granting of access to OPM data systems and are to be followed before granting new access to PII contained in OPM data systems to (1) any U.S. Digital Service (USDS or DOGE) employee, contractor, or detailee, or (2) any OPM employee, contractor, or detailee hired after January 20, 2025, who requires access for the primary purpose of working on an initiative or project involving DOGE. When OCIO identifies an individual in one of the above categories who requires a new grant of access to PII in any OPM data system,[1] an email will be sent to your office (CHCO, FSEM, and CISO) notifying you and your staff about the pending need for the individual to access the specified information. Upon receipt of such notification, please take the following steps and send any applicable documentation or information to both CIO Greg Hogan and Acting Senior Agency Official for Privacy ("SAOP") Becky Ronayne, as pertains to your office:

1- CISO: Please ensure that the person has completed the Privacy and Cybersecurity Awareness training (rules of behavior are included as part of the training), and send to the CIO and SAOP a copy of the training certification and rules of behavior acknowledgment.

[1] OCIO will be responsible for identifying individuals subject to these protocols in the first instance; however, CISO, CHCO, and FSEM should proactively notify OCIO of any individuals who are being onboarded that may fall within these categories of individuals.

2- CHCO: Please confirm that the individual has been properly appointed or detailed, and send copies to the CIO and SAOP of each individual's appointment affidavit, SF-50, and any detail agreement.

3- FSEM: Please confirm that the individual has been appropriately vetted and they have been cleared for entrance on duty; please also provide any credentialing information for their PIV card, as well as any suitability/security clearance, contract agreement (including any non-disclosure agreements that have been executed), and send appropriate supporting documentation demonstrating each the above to the CIO and SAOP.

The individual will receive access to the specified OPM data system(s) containing PII only after the CIO and the SAOP has been notified by the above offices that the appropriate tasks have been completed. In addition, the CIO and SAOP will document the completion of the above steps in a signed memorandum, which will also set forth the Privacy Act provision(s) that allows for access to the specified OPM data system(s), including, when relevant, an explanation of the need for access to PII in performance of the individual's duties.

Please ensure that this memorandum is distributed to all appropriate staff in CISO, CHCO, and FSEM.