CIVIL SERVICE STRONG POWERED BY DEMOCRACY FORWARD

February 10, 2026

Submitted via Federal eRulemaking Portal: https://www.regulations.gov

Scott Kupor, Director
U.S. Office of Personnel Management
1900 E Street, NW
Washington, DC 20415

Subject: Agency Information Collection Request: Federal Employees Health Benefits and Postal Service Health Benefits Programs Service Use and Cost Data, 90 Fed. Reg. 57793 (Dec. 12, 2025)

Dear Director Kupor:

Civil Service Strong ("CSS"), a project of Democracy Forward Foundation, is a national coalition of individuals, organizations, and communities committed to defending and strengthening a nonpartisan, professional civil service. CSS brings together labor organizations, civil society groups, former public servants, and good-government advocates who share the common goal of ensuring that the federal workforce is governed by merit, not politics.

CSS stands committed in supporting the over 2 million civil servants who work tirelessly every day to serve the American people. These civil servants are the backbone of our government—they play a critical role in keeping our food, medicine, transportation, and water safe; securing public safety and national security; delivering our mail; supporting our education and health care systems; ensuring the financial system operates smoothly, and small businesses have access to credit; and working in our courthouses, airports, national parks, and beyond. And these civil servants are worthy of dignity and respect—and to have their rights and privacy protected.

To that end, CSS opposes the Office of Personnel Management's ("OPM") proposed Agency Information Collection Request: Federal Employees Health Benefits and Postal Service Health Benefits Programs Service Use and Cost Data (3206-NEW) (Dec. 12, 2025). The Information Collection Request ("ICR") proposes to allow OPM to collect and maintain highly sensitive medical data on millions of federal employees, federal annuitants, and their family members. This ICR—especially without substantially more detail regarding its purpose and protections—creates a significant risk of abuse, particularly given the Trump-Vance Administration's proclivity for targeting federal civil servants and misusing sensitive data. CSS urges OPM to abandon this harmful and misguided proposal.

I. OPM Fails to Explain How It Will Use This Highly Sensitive Data

First established by Congress in 1959, the Federal Employees Health Benefits Program ("FEHB"), which now includes the Postal Service Health Benefits Program ("PSHB"),[1] is the largest employer-sponsored health insurance program in the country. Through FEHB, OPM contracts with over 60 health insurance carriers to provide health insurance to more than 8 million federal employees, annuitants, and their family members.[2]

Congress entrusted OPM to administer this critical government program—and for decades, OPM has done just that, working to ensure that federal employees and annuitants have access to comprehensive, high-quality, and affordable health insurance for themselves and their families. OPM has been a trusted steward of Congress's creation. But this ICR risks undermining that trust: it would dramatically alter the FEHB landscape, providing OPM with access to data that, without appropriate safeguards, OPM can use for any number of improper purposes. It also lacks assurances that OPM will not share the data with other government agencies for purposes unrelated to administration of the FEHB program.

The ICR indicates OPM's intent to begin collecting "service use and cost data" on enrollees from FEHB health insurance carriers.[3] According to the ICR, this data will include "medical claims, pharmacy claims, encounter data, and provider data." This is highly sensitive data—yet OPM's ICR provides virtually no information, let alone any meaningful explanation, for what OPM plans to do with this data. Instead, the ICR provides only a limited, generic justification that it plans to use the data for "oversight" purposes:

> This data will enable OPM to oversee health benefits programs and ensure they provide competitive, quality, and affordable plans. OPM requires Carriers to report necessary information and permit audits and examinations to manage the FEHB Program effectively.

That is the entirety of OPM's justification for this data collection—and it is entirely insufficient. As an initial matter, the ICR does not identify any legal authority that would allow OPM to collect and maintain this highly sensitive data. But even if this (undisclosed) authority does exist, the only way that OPM can justify such an expansive data collection is to provide substantially more detail regarding its intended use. What specific oversight activities does OPM plan to conduct using this data? How do those oversight activities align with OPM's statutory authorities and mandates? What particular statutory purposes will those oversight activities advance? And, most fundamentally, why is this data necessary for OPM to carry out those activities?

This is not only the minimal information that OPM *should* provide, it is also the minimal information that OPM is *required* to provide. The ICR references HIPAA, the Health Insurance

---

[1] The Postal Service Health Benefits Program (PSHB) is a separate program, created by the Postal Service Reform Act of 2022, that provides health benefit plans to eligible Postal Service employees, annuitants, and eligible family members. PSHB is located within FEHB, and all references to FEHB in this comment are meant to be inclusive of both FEHB and PSHB.

[2] OPM, Federal Employees Health Benefits (FEHB) Program Carriers: Overview, https://www.opm.gov/healthcare-insurance/carriers/fehb/.

[3] 90 Fed. Reg. 57793 (Dec. 12, 2025).

Portability and Accountability Act of 1996, claiming that HIPAA "permits covered entities, including carriers, to disclose protected health information (PHI), including service use and cost data, to health oversight agencies, such as OPM, for oversight activities." But HIPAA's "minimum necessary" standard also requires that an entity requesting or providing such information "make reasonable efforts to limit protected health information to the *minimum necessary* to accomplish the intended purpose of the use, disclosure, or request." 45 CFR 164.502(b) (emphasis added); *see also* 45 CFR 164.514(d) (requirements related to minimum necessary standard).

A similar minimization standard is in the Privacy Act, which governs the federal government's collection, maintenance, use, and dissemination of information about individuals. Specifically, under the Privacy Act, an agency may "maintain in its records only such information about an individual as is relevant or necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order." 5 U.S.C. 552a(e)(1).

Federal law is clear that agencies cannot simply collect data on individuals, much less highly sensitive data like what is at issue in this ICR, for any generic purpose. Instead, agencies may collect and use only that which is minimally necessary to carry out a legally mandated purpose. Here, however, OPM does not provide *any meaningful information* for how it plans to use this data or why the data is necessary for accomplishing such a purpose. Without this explanation, OPM cannot move forward with this expansive and sensitive data collection.

II. OPM Fails to Explain How It Will Properly Safeguard This Highly Sensitive Data

In addition to failing to justify its proposed data collection, OPM's ICR also fails to detail how it will ensure that this highly sensitive data is properly safeguarded and not used for any improper purposes.

As an initial matter, OPM does not state whether the data will be identifiable by individual. If the data is in fact identifiable, then OPM could use it for all manner of improper (and illegal) purposes: discriminating against federal employees based on their health status, targeting them as a result of obtaining certain medical procedures, or threatening to share their (or their family members') protected health information unless they comply with certain demands. The options for harm are near limitless.

And even if OPM does not have any nefarious intent, the ICR's lack of information leaves unanswered the critical question of how OPM will ensure the data is only used for appropriate oversight purposes. Who will have access to the data? How will that access be controlled? What protections and protocols will prevent improper authorization? What security standards will prevent data breaches?

Answers to these questions are the minimal information that OPM must provide. Yet, once again, the ICR does not provide any such answers.

III. The Trump-Vance Administration Has a Disdain for Civil Servants and a Pattern of Abusing Sensitive Data

OPM's ICR is especially concerning given the Trump-Vance Administration's explicit contempt for federal workers and its pattern of recklessness with highly sensitive data.

For starters, President Trump has disparaged career civil servants as "crooked" and "dishonest"[4] and proclaimed that the "deep state must and will be brought to heel," and future Director of the Office of Management and Budget Russell Vought declared that "[w]e want bureaucrats to be traumatically affected."[5] The Administration has followed this rhetoric with action. It has punished civil servants for simply doing their jobs, tried to strip civil service protections from a wide swath of career civil servants, executed significant reductions in force, and retaliated against civil servants who raise concerns about wrongdoing. It requires no leap at all to think that it will now attempt to weaponize federal employees' own medical data against them.

And, of course, the Trump-Vance Administration has made clear that it cannot be trusted with sensitive data. Just a few weeks ago, the government admitted—in contravention of its prior sworn statements—that sensitive Social Security Administration (SSA) data was sent to individuals with no formal relationship with SSA, that an SSA Department of Government Efficiency (DOGE) team member entered into a "Voter Data Agreement" after being asked by a nongovernmental actor to analyze state voter rolls, and that SSA DOGE team members had an unmonitored ability to exchange SSA data on a nongovernmental server.[6] This latest revelation is reflective of a broader pattern of the Administration, and DOGE in particular, playing fast and loose with government data. Needless to say, the Administration's actions to date—coupled with the ICR's paucity of information—provide no comfort that OPM will use FEHB enrollee's medical data in a secure, proper, and lawful way.

***

For each of these reasons, OPM's ICR is woefully insufficient and could lead to serious and lasting harm to federal employees, annuitants, and their family members. CSS urges OPM to abandon this proposal and to instead refocus its efforts on administering the FEHB Program in a manner that honors the commitment and dedication of this country's current and retired civil servants.

---

[4] Erich Wagner, Trump calls federal workforce 'crooked,' vows to hold them 'accountable,' Gov. Exec. (Aug. 28, 2024), https://www.govexec.com/workforce/2024/08/trump-calls-federal-workforce-crooked-vows-hold-them-accountable/399138/; Eric Katz, If Trump Is Reelected, His Aides Are Planning to Purge the Civil Service, Gov. Exec. (July 22, 2022), https://www.govexec.com/workforce/2022/07/trump-reelected-aides-plan-purge-civil-service/374842/.

[5] Alice Herman, Russell Vought: Trump appointee who wants federal workers to be 'in trauma,' The Guardian (Feb. 10, 2025), https://www.theguardian.com/us-news/2025/feb/10/who-is-russell-vought-trump-office-of-management-and-budget.

[6] *American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, et al.*, D. Md., 1:25-cv-00596-EH, Dkt. 197 (Jan. 16, 2026).

Respectfully submitted,

/s/ Robert H. Shriver, III

Robert H. Shriver, III
Managing Director
Civil Service Strong and
Good Government Initiatives