# United States Senate

WASHINGTON, DC 20510

May 16, 2025

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

Dear Mr. Ezell:

I write to bring your attention to a vital issue affecting the federal workforce, past and current, and their families. In 2015, the Office of Personnel Management (OPM) announced two separate cybersecurity incidents. The Social Security numbers, birthdates, and addresses of approximately 21.5 million individuals were compromised in the breaches, including 19.7 million individuals who applied for background investigations and 1.8 million non-applicants (predominantly spouses or cohabitants of applicants).[1] In response to this massive security compromise, I co-sponsored the RECOVER Act, the original bill for OPM-contracted identity protection services for the impacted individuals. [2] Congress appropriated funds in section 633(a) of the Consolidated Appropriations Act of 2017.[3] The Act and appropriation protected the 21.5 million impacted individuals with identity protection coverage and identity theft insurance.[4] This appropriation was "effective for a period of not less than 10 years," and expires at the end of fiscal year 2026, on September 30, 2026.[5]

The 2015 OPM cybersecurity breach was attributed to the People's Republic of China (PRC).[6] In the decade since the breach, the PRC has mounted additional attacks to steal information about America's leaders and public servants to disrupt and endanger the lives of everyday Americans, including recent cyber, critical infrastructure, and telecom security breaches. The federal workforce was dangerously exposed by the 2015 OPM breach, and millions of impacted individuals will continue to be at risk because of the breach, likely for the remainder of their lives. In addition to Social Security numbers, birthdates, and addresses, there were also 1.1 million sets of fingerprints and detailed financial and health records exposed—some of the most valuable information today on the dark web.[7]

The risks and appropriate remedies for the compromise of sensitive information about public servants are well known to this administration. In March 2025, the Trump administration acknowledged the improper disclosure of sensitive information to former public servants when it disclosed the Social Security

---

[1] U.S. Office of Personnel Management. (n.d.). *Cybersecurity Resource Center*. https://www.opm.gov/cybersecurity-resource-center/#url=Overview

[2] U.S. Congress. (2015). *Reducing the Effects of the Cyberattack on OPM Victims Emergency Response Act of 2015 (RECOVER Act), S. 1746, 114th Cong.* https://www.congress.gov/bill/114th-congress/senate-bill/1746

[3] Consolidated Appropriations Act of 2017, Pub. L. No. 115-31, div. E, tit. VI, § 633(a), 131 Stat. 135 (2017)

[4] Consolidated Appropriations Act of 2017, Pub. L. No. 115-31, div. E, tit. VI, § 633(a), 131 Stat. 135 (2017)

[5] Consolidated Appropriations Act of 2017, Pub. L. No. 115-31, div. E, tit. VI, § 633(a), 131 Stat. 135 (2017)

[6] Hanauer, L. (2016, February 1). *OPM hack poses overlooked counterintelligence risk for economic espionage*. RAND Corporation. https://www.rand.org/pubs/commentary/2016/02/opm-hack-poses-overlooked-counterintelligence-risk.html

[7] Nakashima, E. (2015, July 9). *Hacks of OPM databases compromised 22.1 million people, federal authorities say*. The Washington Post. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

numbers, birthdates, and other sensitive information of hundreds of individuals in the release of the files pertaining the death of President John F. Kennedy.[8] To protect those compromised individuals, the Trump administration is reportedly providing credit monitoring and, in some cases, has issued new Social Security numbers to the impacted individuals.[9] While the March 2025 disclosure was a staggering unforced error, I applaud the administration's swift response to protect the victims. Current and former public servants should not be abandoned to bear the risks of the federal government's failure to protect their sensitive information.

It was not practicable to issue millions of new Social Security numbers to the Americans impacted by the 2015 OPM data breach, which is why the federal government responded at the time, followed by Congress appropriating funds to OPM to contract for identity theft protection services. Given the recent personnel cuts to OPM and Elon Musk's imminent departure from the Trump administration, I am deeply concerned that OPM is planning to curtail identity theft monitoring for millions of public servants and their families whose information was compromised in 2015. I urge you to ensure that identity theft protection services for the impacted individuals from the 2015 OPM breach continue, as required by law. Any attempt to prematurely phase out services to the victims of the 2015 OPM breach will introduce tremendous risk to former and current federal employees and create an opportunity for America's adversaries and criminals to target and potentially further compromise millions of Americans.

If you do decide to alter or terminate the current contract(s) protecting over 21 million Americans from identity theft as a result of the 2015 OPM breach, please inform my office and the relevant committees of Congress as soon as you make any such determination.

Sincerely,

Mark R. Warner
United States Senator

[8] Barry, D., & Rosenberg, M. (2025, March 20). *J.F.K. assassination files released with personal information unredacted*. The New York Times. https://www.nytimes.com/2025/03/20/us/jfk-assassination-files-personal-information.html

[9] Barry, D., & Rosenberg, M. (2025, March 20). *J.F.K. assassination files released with personal information unredacted*. The New York Times. https://www.nytimes.com/2025/03/20/us/jfk-assassination-files-personal-information.html