Delivering On Government Efficiency in Spending Act

Bill Summary:

The *Delivering On Government Efficiency (DOGE) in Spending Act* helps secure America's bank account against fraud, waste, and abuse. It requires all payments out of the U.S. Treasury Department (which handles 95% of federal government payments) to have: 1) a brief description of the purpose of the payment, 2) the appropriations account from which the payment is to be drawn, 3) the payment to be reported on USAspending.gov, and 4) an annual update on all information related to ongoing payments.

As an additional quality control measure, it gives Treasury the ability to check relevant databases throughout the government for purposes of confirming eligibility to prevent fraudulent and improper payments. This will break the existing stove piping that enables fraudsters to defraud multiple programs with the same information because government databases do not talk to one another.

Ultimately, this bill codifies the policy reflected in Sections 3 and 4 of President Trump's Executive Order, *Protecting America's Bank Account Against Fraud, Waste, and Abuse.* DOGE estimates this policy could functionally eliminate improper direct payments. GAO reported there were $162 billion in improper payments in Fiscal Year 2024, 84% of which were a result of overpayments.

The Problem:

Prior to DOGE, Treasury did not put even the most essential information into its computer disbursement systems, which led to hundreds of billions of dollars of spending with no ability to account for basic things like why the payments were made. The Treasury Department was also not empowered to double-check agencies' work, leading to hundreds of billions of dollars' worth of fraud and improper payments each year.

In addition, Treasury systems could not check to see if the recipient of a payment out of one program was using the same information to defraud another program. Nor could they determine other information fundamental to preventing mistakes such as whether the SSN or bank account attached to a payment was valid or that it in fact belonged to the payee. Agencies' refusal or inability to share this crucial information with Treasury created a system that enabled bad actors to defraud various programs using the same information, largely without consequence.

How Does the DOGE in Spending Act Fix it?

By requiring agencies to give Treasury's Do Not Pay (DNP) system relevant data before issuing payments, requiring Treasury to code and attach each payment to the relevant appropriations account, and granting Treasury the ability to ping databases at other agencies and available in the private sector to ensure accuracy and eligibility for each payment, we will, for the first time, have a federal payment system equipped with the necessary tools to all but entirely eliminate improper payments and fraud on the front end, and go after any fraudsters who might still slip through the cracks.

Proposal	Context on Why Proposal is Necessary
DNP Access to National Directory of New Hires (NDNH)	◊ The DNP system lacks access to employment and income data, which federal programs often need to determine program eligibility. ◊ By including this data in the DNP system, mandatory federal means-tested programs, such as welfare programs, can rely on DNP, rather than having to acquire the data on a program-by-program basis, which creates potential data quality issues.
DNP Access to Fair Credit Reporting Act (FCRA) Information	◊ The DNP system lacks access to data that is essential for confirming income and location. These data points are necessary for verifying and confirming eligibility for federally funded but state-managed programs, like Medicaid, unemployment insurance, and SNAP. Major credit rating agencies already possess this data. ◊ FCRA data includes name, current and former addresses, credit history, and employment history. ◊ In FY2019, the federal government made $850 million in improper payments without verifying income eligibility for federal benefits. ◊ Incorporating FCRA data into the DNP system would permit programs to engage in fraud prevention based on residency and income eligibility.

DNP Limited Access to Select Tax Information	◊ The DNP system lacks access to certain tax data pursuant to 26 U.S.C. § 6103, which would help the Bureau of Fiscal Service identify, prevent, and mitigate fraud. This includes:
	  ◊ Taxpayer Identity Information (TIN);
	  ◊ Filing status;
	  ◊ AGI;
	  ◊ The amount reported on Schedule C of Form 1040 (or an equivalent successor schedule);
	  ◊ Filing year;
	  ◊ Bank account information;
	  ◊ Reported identity theft associated with a TIN; and
	  ◊ Whether a tax return was not filed for a taxable year.
	◊ This proposal **does not** provide substantive tax information on a general basis. The language carefully authorizes an IRS response to specific inquiries from BFS in a manner consistent with IRS privacy protection laws. Ex: Was Jane Doe's AGI less than or equal to $X in year 2024?

DNP Access to Social Security Information	◊ Currently, DNP lacks access to the Social Security Number (SSN) and TIN associated with each beneficiary, a requirement under Executive Order 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse*. ◊ Giving the DNP system access to this information enables verification of basic applicant information (name, DOB, SSN) for applicant eligibility and to prevent program or identity fraud. ◊ SSA already provides SSN validation to private financial institutions for identity fraud prevention, as required by the *Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018*. However, Congress did not make the same data available to federal agencies or the DNP system.

For more information, please contact aaron_gottesman@ernst.senate.gov.