U.S. Department of Labor
Office of Inspector General
Audit

BRIEFLY...

DOL NEEDS TO DO MORE TO SECURE EMPLOYEES' PERSONALLY IDENTIFIABLE INFORMATION IN THE TRAVEL MANAGEMENT SYSTEM

September 10, 2020

WHY OIG CONDUCTED THE REVIEW

DOL's travel management system, E2 Solutions (E2), is managed by the Office of the Chief Financial Officer (OCFO) and contains personally identifiable information (PII) for all DOL employees who use the system. PII in E2 includes highly sensitive information, such as employees' social security numbers and credit card numbers, which are common targets for identity theft. E2 also has sensitive details regarding DOL personnel's travel plans.

Concerned by the potential risk of unauthorized access to or unintentional exposure of employees' PII, we reviewed OCFO's management of E2.

WHAT OIG DID

We conducted a review to answer:

> Did DOL effectively manage its E2 travel system to prevent unnecessary access to DOL employees' PII?

To determine this, we conducted interviews and reviewed relevant DOL policies and procedures, federal laws, regulations, contract requirements, and E2 user account permissions.

REPORT NUMBER: 23-20-003-13-001

WHAT OIG FOUND

DOL did not effectively manage its E2 travel system to prevent unnecessary access to DOL employees' PII, as the OCFO did not manage E2 user accounts according to DOL information security policies.

We found the OCFO had not provided sufficient guidance to agencies' personnel for securing E2 user accounts during creation and account maintenance. Additionally, the OCFO had not performed the oversight necessary to ensure E2 user accounts were appropriately created and maintained. Furthermore, we found the OCFO had not fully implemented the E2's contractual security requirements and deliverables.

These conditions existed as the OCFO had not implemented controls to appropriately manage E2 user accounts and contractual requirements. By the OCFO not ensuring E2 user accounts were appropriately secured, DOL employees were found at risk of having their PII accessed.

WHAT OIG RECOMMENDED

We recommended the Chief Financial Officer:

1. Establish and implement procedures to ensure E2 account management practices enforce DOL's security policies.

2. Establish and implement procedures to ensure E2 is managed in compliance with contractual security requirements and DOL computer security policies for contracted information systems.

OCFO agreed with the our recommendations and has already initiated some actions to address these recommendations.

READ THE FULL REPORT

The DOL OIG sometimes issues a report containing sensitive information, and may redact certain information or in some instances, because of the highly sensitive nature of the entire report, the OIG may not make the report publicly available. In those instances, a brief summary of the report is posted to the website, which is the case here.