Report in Brief
Date: March 2024
Report No. A-18-22-03200

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

ACF Has Enhanced Some Cybersecurity Controls Over the Unaccompanied Children Portal and Data But Improvements Are Needed

Why OIG Did This Audit

The Unaccompanied Children (UC) Program has experienced heightened attention and oversight from OIG and the Government Accountability Office. In a prior audit report of the Administration for Children and Families (ACF), we reported that ACF did not adequately implement controls over the UC Portal to protect sensitive data in accordance with Federal requirements. During that audit, our penetration test identified vulnerabilities with ACF's UC Portal application. We conducted the current audit because OIG believes vulnerabilities in ACF's controls over UC data may still exist.

Our objectives were to determine if ACF: (1) sufficiently addressed our prior audit findings, (2) implemented controls to ensure the cybersecurity of sensitive UC data in accordance with Federal requirements, and (3) incorporated adequate system development life cycle (SDLC) planning to ensure that the UC Portal aligns with its business and performance objectives.

How OIG Did This Audit

We assessed general IT controls and ACF's implementation of our prior audit recommendations. To accomplish this, we reviewed ACF's policies and procedures, interviewed staff, and reviewed the UC system security plan. We also reviewed ACF responses to the prior audit report and ACF's actions taken to address the findings. Finally, we assessed the ACF system development practices for the UC portal.

What OIG Found

ACF implemented six of our seven prior audit recommendations by enhancing some of the cybersecurity controls that protect the sensitive UC Portal and data. The recommendation that was not completely addressed focused on user account reviews. Specifically, ACF did not consistently perform the reviews in accordance with the access control policy it issued in response to our prior audit recommendation. Also, ACF implemented 119 of 159 minimum required controls for a moderate system to ensure the cybersecurity of sensitive UC data. Of the remaining 40 cybersecurity controls, ACF did not fully implement 30 controls and designated 10 controls as "not applicable." Finally, ACF performed adequate SDLC planning to ensure that the UC Portal aligns with its business and performance objectives.

What OIG Recommends and ACF Comments

We recommend that the ACF: (1) consistently perform user account reviews in accordance with its access control policy and (2) fully implement the 30 required minimum controls identified in the UC Portal system security plan in different stages of implementation.

In written comments, ACF concurred with our recommendations and described actions that it has taken or planned to take implement them, including its rollout of a single sign-on application slated for completion after full integration with the Department of Homeland Security's identity system. ACF also stated that it implemented or is in process of implementing the required minimum controls identified in the UC Portal system security plan in different stages of implementation.