Report in Brief
Date: August 2019
Report No. A-18-18-06001

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

Southwest Key Did Not Have Adequate Controls in Place To Secure Personally Identifiable Information Under the Unaccompanied Alien Children Program

Why OIG Did This Review

As part of the Department of Health and Human Services' (HHS's) Administration for Children and Families (ACF), the Office of Refugee Resettlement (ORR) manages the Unaccompanied Alien Children (UAC) program. ORR awards funds, primarily through grants, to organizations to provide residential care to UAC.

Our objective was to assess whether Southwest Key had implemented an adequate information systems security program to protect the personally identifiable information (PII) of UAC.

How OIG Did This Review

We reviewed information system general controls at Southwest Key, including logical access, mobile and wireless device management, risk assessment, vulnerability management, and virtual machine management. To accomplish our objective, we used appropriate procedures from applicable Federal requirements and guidance. We performed our audit field work from November 2017 through September 2018.

What OIG Found

Southwest Key had not implemented an adequate information systems security program to protect the PII of UAC. Southwest Key officials explained that they were unaware of information systems security requirements from ORR or other Federal requirements. Based on the control areas we reviewed, we determined that Southwest Key's security program lacked several fundamental security controls needed to protect the confidentiality, integrity, and availability of UAC Program PII as required by 45 CFR section 75.303(e). Without fundamental information systems security controls (e.g., having an information systems security officer, a risk assessment, and an information systems security awareness training program), Southwest Key management cannot ensure that it has established a control environment that meets minimal information security requirements as required by Federal regulations to safeguard the UAC program PII from both internal and external threats.

What OIG Recommends and Southwest Key Comments

We recommend that Southwest Key management develop and implement an information systems security program in accordance with Federal requirements. We also recommend that Southwest Key communicate with ORR, ACF, and HHS to obtain Federal security requirements and guidance to improve its security posture and protect UAC PII.

In written comments on our draft report, Southwest Key generally concurred with the spirit of our recommendations while disputing the corresponding findings, one pertaining to information security awareness training and another pertaining to reviews of user access privileges. We maintain that our recommendations are valid.

Southwest Key did not agree that National Institute of Standards and Technology (NIST) guidelines applied to its IT environment because those standards had never been invoked through ORR or ACF guidance or Federal award requirements. However, Southwest Key stated that it would communicate with ORR and ACF regarding information security requirements. Although ACF grant regulations do not explicitly specify a standard for IT security, NIST guidelines are the Federal industry standard in accordance with the Federal Information Security Modernization Act of 2014 (FISMA); therefore, because Southwest Key maintains UAC records, which are the property of ORR and ACF, to comply with FISMA, we recommend that Southwest Key use NIST guidelines.