Department of Health and 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

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Joanne Chiedi
Acting Inspector General

August 2019
A-18-18-06001

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nation-wide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the healthcare industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG website.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

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.

TABLE OF CONTENTS

INTRODUCTION

WHY WE 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 UACs. The Office of Inspector General (OIG) selected grantee Southwest Key Programs (Southwest Key) for this review because of information systems security risks observed onsite during another separate OIG audit.[1]

OBJECTIVE

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.

BACKGROUND

The HHS Unaccompanied Alien Children Program

On March 1, 2003, section 462 of the Homeland Security Act of 2002 transferred responsibilities for the care and placement of UAC from the Commissioner of the Immigration and Naturalization Service to the Director of the ORR. Since then, ORR has cared for more than 175,000 children, incorporating child welfare values as well as the principles and provisions established by the Flores Agreement in 1997, the Trafficking Victims Protection Act of 2000, and its reauthorization acts (the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2005 and 2008).

[1] The OIG is conducting audits of grantees assessing their compliance with applicable health and safety standards and financial requirements. This series of audits was undertaken because of the rapid increase of vulnerable children entering ORR care, the significant increases in program funding, and multiple changes to ORR policies during FY 2014. OIG Workplan Item W-00-17-25060 (Office of Refugee Resettlement, Unaccompanied Alien Children Program—Review of Selected Grantees Nationwide).

Office of Refugee Resettlement

The UAC program funds temporary shelter care[2] and other related services for UAC in ORR custody. For project periods[3] with services beginning during FY 2014 and FY 2015, ORR awarded grants totaling $2.1 billion to providers for the care and placement of children. The UAC program is separate from State-run child welfare and traditional foster care systems.

Southwest Key Programs

Founded in 1987, Southwest Key is a non-profit social service, education, and community development organization administering program areas such as immigrant children's shelters and youth justice alternatives to detention or incarceration. Southwest Key's national headquarters is in Austin, Texas, and it has program locations in Arizona, California, and Texas.

Federal Requirements and Guidance

Federal regulations (45 CFR § 75.303) states that the non-Federal entity must: (a) Establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award… and (e) Take reasonable measures to safeguard protected personally identifiable information and other information the HHS awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality. In addition, we used for guidance National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*; NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View;* and NIST SP 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise.*

HOW WE CONDUCTED THIS REVIEW

We reviewed information system general controls at Southwest Key, including logical access, mobile and wireless device management, risk assessment, vulnerability management, and

[2] Shelter care is a residential care provider facility in which all of the programmatic components (such as the shelter, food, education, and medical services provided as part of the UAC program) are administered onsite in the least restrictive environment. When making placement determinations, ORR's goal is to provide the least restrictive setting that is in the best interests of the child, taking into consideration certain factors such as potential flight risk and danger to the child and others.

[3] A project period for the UAC program is a 36-month project with three 12-month budget periods.

virtual machine management. To accomplish our objective, we used appropriate procedures from applicable Federal requirements and guidance. Appendix B contains specific Federal criteria.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We shared with Southwest Key information about our findings in advance of issuing our draft report.

Appendix A contains the details of our audit scope and methodology.

FINDINGS

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 § 75.303(e).

Specifically, Southwest Key's information systems security program did not:

- have an individual in place responsible for information systems security, such as an information systems security officer (ISSO);
- have an entity-wide information systems risk assessment;
- have an information systems security awareness training program;
- have formal security control policies and procedures over its mobile and wireless network management program;
- conduct reviews of user access privilege of its [redacted] to ensure compliance with NIST least privilege requirements[5]; and

[redacted]s a software program designed for data management of UAC PII.

[5] The principle of least privilege ensures that the level of access granted is no greater than what is required (NIST Special Publication (SP) 800-53, Revision 4, Section AC-6).

- have formal procedures for conducting vulnerability scans of its network and other systems storing PII.

Without fundamental information systems security controls, such as having an ISSO, 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 UAC program PII from both internal and external threats.[6]

Southwest Key Needs an Individual Responsible for Information Systems Security

Southwest Key did not designate an individual responsible for systems security, such as an ISSO, to ensure a managed and implemented organization-wide information systems security program. NIST guidelines recommend the appointment of an information security officer to coordinate, develop, implement, and maintain an organization-wide information systems security program.[7] Additionally, Federal guidelines state that the ISSO is responsible for their organizations' security programs, including risk management.[8] ISSOs are responsible for ensuring that an appropriate operational security posture is maintained for a system. Other ISSO responsibilities include (but are not limited to) assisting in the development of information security policies and procedures, overseeing the day-to-day information security operations of the system, and ensuring that the system complies with information security policies and procedures. ISSOs also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis.

Southwest Key recognizes the need for an ISSO; it has posted a job announcement and is actively seeking to fill the position.

Southwest Key Did Not Conduct a Risk Assessment for Its Information Systems

Southwest Key did not conduct an information systems risk assessment. The risk assessment is used to determine the extent of the potential threats and risks associated with an information system. An effective risk management process is an important component of a successful

[6] 45 CFR § 75.303.

[7] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* Section PM-2.

[8] NIST SP 800-30, *Guide for Conducting Risk Assessments.* Section 2.3.

information technology (IT) security program.[9] Southwest Key stated that it was in the process of conducting a risk assessment and had provided a vulnerability scan of its network at the end of our audit fieldwork in September 2018; however, the scan itself does not fully meet Federal guidelines for a complete risk assessment.[10] Without a completed risk assessment, Southwest Key cannot fully ensure that management has sufficient risk information to protect information systems that are subject to threats such as [redacted]

Southwest Key Did Not Have an Information Systems Security Awareness Training Program

Southwest Key did not have an information systems security awareness training program. Information systems security awareness training is a key control to reduce risks from human error; in addition, a signed rules of behavior informs users and holds them accountable for their actions while utilizing organizational IT resources.[11] Southwest Key management was unaware of requirements for having an information systems security awareness training program. Failure to give attention to information systems security awareness puts an organization at risk and is as much a human issue as it is a technology issue.[12] Without an information systems security awareness training program, Southwest Key management cannot effectively hold users accountable and ensure that they are aware of their responsibilities while using the organization's IT equipment. After our audit fieldwork, Southwest Key officials stated that they had developed and implemented an information systems security awareness training program.

Southwest Key Did Not Have a Mobile and Wireless Device Security Management Program

Southwest Key did not have adequate security control polices or procedures over its mobile and wireless device management program. Federal guidelines state that each organization should make its own risk-based decisions about what levels of access should be permitted from which types of mobile devices.[13] Southwest Key officials stated that Southwest Key was still assessing which information systems security control options were available within its mobile and

[9] NIST SP 800-30. Section 1.

[10] See also NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

[11] NIST SP 800-30. Section 2.3.

[12] https://www.techrepublic.com/article/over-40-of-reported-security-breaches-are-caused-by-employee-negligence/. Accessed on January 7, 2018.

[13] NIST SP 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Section 4.1.1.

wireless security software to apply to its environment. Specifically, we found that Southwest Key:

Without an adequate mobile and wireless management program, Southwest Key cannot ensure the protection of the confidentiality, integrity, and availability of sensitive UAC program information on mobile and wireless devices. After our fieldwork was completed, Southwest Key stated that it was in the process of hiring a vendor to securely configure, test, and deploy an MDM system but had no estimated time of completion.

Southwest Key Did Not Review User Access Privileges

Southwest Key officials informed us that they did not conduct reviews of user access privileges for its system. Federal guidelines state that the organization review the privileges assigned to users to validate the need for such privileges and reassign or removes privileges as necessary.[15] Southwest Key officials stated that they were unaware of Federal guidelines for reviewing user access privileges. Without reviewing user access privileges, Southwest Key might be giving employees access to systems they do not need and allowing more than the least privileges required to complete a user's assigned job functions.

[15] NIST SP 800-53, Revision 4. Appendix F-AC.

After our fieldwork was completed, Southwest Key officials informed us that it was implementing access control procedures in conjunction with adding security software to ensure that its users are restricted to least privilege access.

Southwest Key Did Not Conduct Vulnerability Scans of Its Network

Southwest Key did not conduct vulnerability scans of its network to help ensure that it was not vulnerable to hackers. Federal guidelines recommend scans for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system or applications are identified and reported.[16] Southwest Key was unaware of any Federal requirements for conducting information systems vulnerability scans. Without information systems vulnerability scanning, Southwest Key management can only react to situations such as ransomware and cyberattacks rather than being proactive about prioritizing, addressing, and remediating vulnerabilities to minimize impact to business operations, including privacy and security.

After our fieldwork, Southwest Key provided the results of a vulnerability scan of its network and was in the process of addressing and remediating all identified vulnerabilities. Southwest Key officials stated that they were waiting to develop formal procedures for a vulnerability assessment program because they said it is an ISSO decision.

RECOMMENDATIONS

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.

Additionally, we recommend that Southwest Key:

1. continue to pursue hiring an ISSO, or assess the risks of not having an individual responsible for information systems security and determine the risk acceptance levels,

2. conduct an entity-wide risk assessment in accordance with Federal requirements and guidance,

3. develop and implement an information systems security awareness training program that meets NIST guidelines,

[16] NIST SP 800-53, Revision 4. Section RA-5.

4. develop and implement formal information security control policies and procedures over its mobile and wireless management programs,

5. complete the implementation of software to address least privilege access and conduct reviews of user access privileges for its [redacted] system to ensure that Southwest Key fully complies with Federal least privilege principles, and

6. develop and implement formal procedures for conducting vulnerability scans of its network and other systems storing PII.

SOUTHWEST KEY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, Southwest Key did not agree that 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, the grant announcement states: "Applicants must provide documentation of a system that preserves the confidentiality of UAC information and protects the records from unauthorized use or disclosure. The records of UAC are the property of ORR and are required to be provided to ORR upon request." NIST guidelines are the Federal industry standard in accordance with the Federal Information Security Modernization Act of 2014 (FISMA)[17]; therefore, because Southwest Key maintains UAC records that are the property of, and on the behalf of ORR and ACF, to comply with FISMA, we recommend that Southwest Key use NIST guidelines.

Southwest Key generally concurred with the spirit of our recommendations while disputing the corresponding finding—specifically, finding #3, recommending an information systems security awareness training program, and finding #5, recommending reviews of user access privileges of its [redacted] system to ensure compliance with NIST least privilege requirements. Regarding finding #3, Southwest Key stated that it had a security awareness training course called KnowB4 and is in the process of making this course mandatory; however, during our audit, Southwest Key officials informed us that an information security awareness training program had not been developed. Southwest Key officials provided us with the KnowB4 security awareness training course after the audit fieldwork was completed, but we could not verify whether this course met NIST guidelines because we were not given access to the entire course due to vendor restrictions. In addition, Southwest Key officials informed us that they were waiting on the new ISSO to verify whether the KnowB4 security awareness training course met NIST guidelines;

[17] FISMA requires federal agencies, such as ACF, to identify and provide appropriate information security for (1) information collected or maintained on behalf of the agency or (2) information systems used or operated by an organization on behalf of the agency. FISMA also requires the agency to secure its systems in accordance with NIST SP 800-53 guidelines.

therefore, we continue to recommend that Southwest Key develop and implement an information systems security awareness training program that meets NIST guidelines.

Regarding finding #5, Southwest Key stated that it had conducted reviews of user access privileges and had mitigating controls to provide for adequate security. However, during our audit and after multiple requests, Southwest Key officials did not provide documentation to support that user access privilege reviews on the [redacted] system were being conducted. Southwest Key also stated that it is implementing a new system to replace the current [redacted] system and is adding role-based access for more security. We recommend that Southwest Key document and maintain its reviews of user access privileges.

Southwest Key's comments are included as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed information systems general controls at Southwest Key, including logical access, mobile and wireless device management, risk assessment, vulnerability management, and virtual machine management.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal criteria, NIST guidance, and Southwest Key policies and procedures;
- reviewed Southwest Key documentation to support its existing controls;
- interviewed Southwest Key awardee staff to discuss internal policies and procedures for securing information systems;
- assessed Southwest Key policies and procedures for applicable audit areas;
- analyzed supporting documentation such as logical access reports;
- judgmentally selected user accounts to review to determine whether users accessed the [redacted] system after termination;
- discussed our findings with Southwest Key officials; and
- performed our fieldwork from November 2017 through September 2018.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: FEDERAL CRITERIA

Code of Federal Regulations

Federal regulations (45 CFR § 75.303) states that the non-Federal entity must:

> (a) Establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award. These internal controls should be in compliance with guidance in "Standards for Internal Control in the Federal Government," issued by the Comptroller General of the United States or the "Internal Control Integrated Framework," issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
>
> (b) Comply with Federal statutes, regulations, and the terms and conditions of the Federal awards.
>
> (c) Evaluate and monitor the non-Federal entity's compliance with statutes, regulations and the terms and conditions of Federal awards.
>
> (d) Take prompt action when instances of noncompliance are identified including noncompliance identified in audit findings.
>
> (e) Take reasonable measures to safeguard protected personally identifiable information and other information the HHS awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.

United States Government Accountability Office

According to the *Standards for Internal Control in the Federal Government* (September 2014):

> Having established an effective control environment, management assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.
>
> - Management assesses the risks the entity faces from both external and internal sources.

Management should define objectives clearly to enable the identification of risks and define risk tolerances.

- Management should identify, analyze, and respond to risks related to achieving the defined objectives.

- Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

- Management should identify, analyze, and respond to significant changes that could impact the internal control system.

- Management evaluates security threats to information technology, which can be from both internal and external sources. External threats are particularly important for entities that depend on telecommunications networks and the Internet. External threats have become prevalent in today's highly interconnected business environments, and continual effort is required to address these risks. Internal threats may come from former or disgruntled employees. They pose unique risks because they may be both motivated to work against the entity and better equipped to succeed in carrying out a malicious act as they have greater access to and knowledge of the entity's security management systems and processes.

National Institute of Standards and Technology Special Publications

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Section RA-5, recommends:

> The organization:
>
> a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
>
> b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
>
> 1. Enumerating platforms, software flaws, and improper configurations;
> 2. Formatting checklists and test procedures; and
> 3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

NIST SP 800-53, Revision 4, Section AC-6, recommends that the organization periodically reviews the privileges assigned to users, validates the need for such privileges, and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* (October 2003), "identifies the four critical steps in the life cycle of an IT security awareness and training program:" (1) Awareness and Training Program Design, (2) Awareness and Training Material Development, (3) Program Implementation, and (4) Post-Implementation. (See also NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.)*

NIST SP 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, Section 4.1.1 Restrictions on Mobile Devices and Access Levels, recommends that:

> Each organization should make its own risk-based decisions about what levels of access should be permitted from which types of mobile devices. For example, an organization might permit only organization-owned mobile devices to be used. Some organizations have tiered levels of access, such as allowing organization-issued mobile devices to access many resources, BYOD mobile devices running the organization's mobile device management client software to access a limited set of resources, and all other BYOD mobile devices to access only a few web-based resources, such as email. This allows an organization to limit the risk it incurs by permitting the most-controlled devices to have the most access and the least-controlled devices to have only minimal access. Some organizations also maintain lists of approved mobile devices (by operating system version, by brand/model of phone, etc.)

NIST SP 800-124, Revision 1, Section 4.2 Development, recommends that the organization consider "how incidents involving the mobile device solutions should be handled and document those plans as well."

Major considerations include the following:

- Architecture. Designing the architecture includes the selection of mobile device management server and client software, the placement of the mobile device management server and other centralized elements, and the architecture of any virtual private network (VPN) solutions.

- Authentication. Authentication involves selecting device and/or user authentication methods, including determining procedures for issuing and resetting authenticators and for provisioning users and/or client devices with authenticators (see "Device provisioning" below). Authentication includes access to or integration with existing enterprise authentication systems.

- Cryptography. Decisions related to cryptography include selecting the algorithms for encryption and integrity protection of mobile device communications and setting the key strength for algorithms that support multiple key lengths. Federal agencies must use [Federal Information Processing Standards] FIPS-approved algorithms contained in validated cryptographic modules when using cryptography to protect information.

- Configuration requirements. This involves setting minimum security standards for mobile devices, such as mandatory host hardening measures and patch levels, and specifying additional security controls that must be employed on the mobile device, such as a VPN client.

- Device provisioning. It is important to determine how both new and existing devices will be provisioned with client software, authenticators, configuration settings, etc.

- Application vetting and certification requirements. This sets security, performance, and other requirements that applications must meet and determines how proof of compliance with requirements must be demonstrated.

APPENDIX C: RELATED OFFICE OF INSPECTOR GENERAL REPORTS

Report Title	Report Number	Date Issued
The Children's Village, Inc., an Administration for Children and Families Grantee, Did Not Always Comply With Applicable Federal and State Policies and Requirements	A-02-16-02013	4/26/2019
Lincoln Hall Boys' Haven, an Administration for Children and Families Grantee, Did Not Always Comply With Applicable Federal and State Policies and Requirements	A-02-16-02007	2/11/2019
BCFS Health and Human Services Did Not Always Comply With Federal and State Requirements Related to the Health and Safety of Unaccompanied Alien Children	A-06-17-07007	12/6/2018
Florence Crittenton Services of Orange County, Inc., Did Not Always Claim Expenditures in Accordance With Federal Requirements	A-09-17-01002	10/15/2018
Heartland Human Care Services, Inc., Generally Met Safety Standards, But Claimed Unallowable Rental Costs	A-05-16-00038	9/20/2018
Florence Crittenton Services of Orange County, Inc., Did Not Always Meet Applicable Safety Standards Related to Unaccompanied Alien Children	A-09-16-01005	6/18/2018
BCFS Health and Human Services Did Not Always Comply With Federal Requirements Related to Less-Than-Arm's-Length Leases	A-06-16-07007	2/20/2018
Office of Refugee Resettlement Unaccompanied Alien Children Grantee Review—His House	A-04-16-03566	12/4/2017

APPENDIX D: SOUTHWEST KEY COMMENTS

southwest key programs

National Headquarters
6002 Jain Lane, Austin, Texas 78721
phone: 512.462.2181 • fax: 512.462.2028 • www.swkey.org

May 21, 2019

Amy J. Frontz
Assistant Inspector General for Audit Services
U.S. Department of Health and Human Services
Office of Inspector General
Washington, DC 20201

Subj: Comments Regarding Draft Report No. A-18-18-06001

Dear Ms. Frontz:

Southwest Key Programs ("SWK") appreciates the opportunity to comment on the above-referenced draft Office of Inspector General ("OIG") report. We acknowledge and appreciate that federal regulations require SWK to "[t]ake reasonable measures to safeguard protected personally identifiable information ["PII"] and other information the HHS awarding agency . . . designates as sensitive . . ."[1]

Though we concur with the general intent of the draft report's findings, we believe it important to note that SWK has long maintained security measures on its information technology systems. To the extent the draft report implies the National Institute of Standards and Technology ("NIST") publications[2] operated as binding requirements within Office of Refugee Resettlement ("ORR") programs, or as binding requirements upon federal grantees generally, we do disagree. Such standards have, to our knowledge, never been invoked through any ORR or Administration for Children and Families ("ACF") guidance, nor are they invoked as binding references within the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (the "Uniform Guidance").[3]

[1] 45 C.F.R. § 75.303(e).

[2] NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*; NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; and NIST SP 800 800-124 *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.

[3] By comparison, 45 C.F.R. § 75.303(a) specifically invokes the GAO Green Book and Committee of Sponsoring Organizations of the Treadway Commission ("COSO") guidelines, § 75.302 specifically invokes Generally Accepted Accounting Principles ("GAAP"), § 75.474(d) specifically invokes federal travel reimbursement standards, § 75.450(c)(2)(iv) cross references specific Internal Revenue Code standards, and § 75.501 specifically invokes the Generally Accepted Government Accounting Standards ("GAGAS," or the "GAO Yellow Book").

southwest key programs

National Headquarters
6002 Jain Lane, Austin, Texas 78721
phone: 512.462.2181 • fax: 512.462.2028 • www.swkey.org

Though we disagree with the implication that the items identified by the OIG constituted, in any way, violations of regulatory requirements, we (i) do take them seriously, (ii) have begun to implement remedial measures, and (iii) propose implementing further such measures. With full concurrence regarding the importance of security, preparedness and constant quality improvement, we address the draft report's findings and recommendations below.

Comments on Draft Findings

1. Individual Responsible for Information Systems Security.

Based upon NIST guidance, the draft report states that SWK should formally designate an individual as its Information Systems Security Officer ("ISSO").[4] We are pleased to report that SWK has hired a new Director of Information Technology who has experience as an ISSO and who is currently providing system security oversight as one of his duties. SWK intends to further hire an additional individual to serve formally in the role of SWK ISSO and is working to contract for ISSO services in the interim.

While SWK had not previously formally established an ISSO position, there have been individuals within its information technology department since 2007 providing information systems security oversight.

[redacted]

2. Information Systems Risk Assessment.

The draft report asserts that while SWK conducted a network vulnerability scan, it "did not conduct an information systems risk assessment" that met standards promulgated by NIST for "a complete assessment."[5]

SWK continued its work in this area after the audit fieldwork was completed, accomplishing a risk assessment for our corporate domain that met NIST technical standards in 2018. We are in the process of implementing remedial measures to address findings from that assessment. Further, SWK is presently in the process of contracting for an additional risk assessment that will meet all NIST standards for all locations.

3. Information Systems Security Awareness Training Program.

[4] Draft Report at 4.

[5] Draft Report at 5.

southwest key programs

National Headquarters
6002 Jain Lane, Austin, Texas 78721
phone: 512.462.2181 • fax: 512.462.2028 • www.swkey.org

The draft report asserts that SWK "did not have an information systems security awareness training program."[6] SWK did, in fact, have a security awareness training course, referred to internally as "KnowB4," that was available to all employees and completed by approximately one-third of them. We concur that this training course should be a required course as opposed to voluntary and are in the process of making this particular training module a mandatory item for all SWK employees.

4. Mobile and Wireless Device Security Management Program.

The draft report asserts that SWK "did not have adequate security control policies or procedures over its mobile and wireless device[s]."[7] We concur generally with the draft report's assertion that systems should provide for: [redacted]

SWK is in the process of evaluating vendors for implementation of these tools and standards to the extent they may not already be in place at SWK. Our existing measures and tools do include [redacted]

5. Review of User Access Privileges.

The draft report asserts that SWK "might be giving employees access to systems they do not need and allowing more than the least privileges required to complete a user's assigned job functions."[8] In particular, the report asserts that SWK failed to adequately restrict privileges to its [redacted] system.

We disagree with this finding as stated. While we concur that regular reviews of system privileges are an important security measure, we believe our [redacted] system privileges were sufficiently narrow to provide for reasonable security. Specifically, for [redacted] (i) only employees with a business/job-function need for access to the system are provided accounts, (ii) access is limited by user to the files associated with unaccompanied minors at only the specific geographic site where the user is providing services, (iii) SWK revokes access privileges immediately upon termination of employment, and (iv) SWK conducts monthly user reviews which result in deactivation of accounts that have been inactive for seventy-five days.

[6] *Id.*

[7] Draft Report at 6.

[8] Draft Report at 7.

southwest key programs

National Headquarters
6002 Jain Lane, Austin, Texas 78721
phone: 512.462.2181 • fax: 512.462.2028 • www.swkey.org

For a number of reasons, we are implementing a new software system to replace [redacted] The new system will enable additional narrowing of system access by user job-function. For example, beyond limiting access to files by geographic employment site, we will be able to limit clinician access to only clinical files, caseworker access to only case management files, *etc.*

6. Network Vulnerability Scans.

The draft report asserts that SWK "did not conduct vulnerability scans of its network to ensure that it was not vulnerable to hackers."[9] We concur in general terms that vulnerability scans are an important safety measure. The draft finding is confusing, however, as the second draft finding above (regarding "risk assessments") acknowledged that SWK had conducted a vulnerability scan in 2018. It is our intent moving forward to conduct such scans annually.

In any event, we concur that SWK will benefit from implementing additional measures to assess and mitigate unauthorized access vulnerabilities. We are in the process of researching and evaluating and will make any corrective actions necessary moving forward.

Comments on Draft Recommendations

To the extent the draft report encourages SWK to continue to undertake all measures necessary to strengthen its information system security and maintain protections for PII and other sensitive information, we concur. Further, as recommended in the draft report, we will communicate with ORR and ACF about requirements and expectations relating to protection of such information.

Conclusion

SWK is committed to compliance with all federal requirements and the safeguarding of information related to the unaccompanied minors in our care. We are happy to answer any questions you may have. Moreover, we look forward to working with ORR to ensure our programs continue to meet the government's expectations in all respects.

I may be reached anytime at (512) 462-2181 or by email at the address you have on file.

Sincerely,

[9] *Id.*

southwest key programs

National Headquarters
6002 Jain Lane, Austin, Texas 78721
phone: 512.462.2181 • fax: 512.462.2028 • www.swkey.org

Joella Brooks
Interim Chief Executive Officer

cc: Stephen Calvert, Chief Legal and Administrative Officer, SWK