Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

ACF HAS ENHANCED SOME CYBERSECURITY CONTROLS OVER THE UNACCOMPANIED CHILDREN PORTAL AND DATA BUT IMPROVEMENTS ARE NEEDED

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

Amy J. Frontz
Deputy Inspector General
for Audit Services

March 2024
A-18-22-03200

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

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. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, 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: 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.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

Unaccompanied children (UC) are a vulnerable population in the custody of the Office of Refugee Resettlement (ORR), a program office of the Administration for Children and Families (ACF). ORR collects data related to each child to assist in caring for the child while in ORR custody and in identifying a suitable sponsor in the United States who can care for the child when he or she leaves ORR custody. The data must be protected, accurate, and accessible to authorized users. Unauthorized modification of UC data could lead to errors in providing educational, legal, and medical services or possible misplacement of UC with incorrect sponsors. The cybersecurity of UC data relies on effective controls that can prevent and mitigate loss or unauthorized exposure of the data.

The UC Program has experienced heightened attention and oversight from the Office of Inspector General (OIG) and the Government Accountability Office. In a prior audit report, OIG 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—a simulation of real-world cyberattacks by experts to test ACF's security controls—identified vulnerabilities with ACF's UC Portal application.[1] Those results also demonstrated that UC data were at risk. We conducted the current audit because OIG believes vulnerabilities in ACF's controls over UC data may still exist.

OBJECTIVES

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.

BACKGROUND

The Unaccompanied Children Program

The Homeland Security Act of 2002 transferred the responsibilities for the care and placement of UC to ORR from the former Immigration and Naturalization Service to move toward a child-welfare-based model of care and away from the adult detention model. Federal law requires that each child in the UC Program be promptly placed in the least restrictive setting that is in the best interest of the child, subject to considerations of whether the child is a danger to self or others.

[1] *The Administration for Children and Families Did Not Adequately Implement Controls Over the Unaccompanied Alien Children Portal to Protect Sensitive Data in Accordance with Federal Requirements* (A-18-19-06002), issued Dec. 10, 2020.

UC are referred to ORR by other Federal agencies, usually the Department of Homeland Security (DHS). Most children are placed into ORR care because they were apprehended by immigration authorities while trying to cross the United States border; others are referred after coming to the attention of immigration authorities at some point after crossing the border. The UC Program serves minors who arrive in the U.S. unaccompanied, as well as minors who, after entering the country, are separated from their parents or legal guardians by immigration authorities. HHS plays no role in the apprehension or initial detention of UC prior to their referral to HHS custody, and HHS is not party to the child's immigration proceedings. The population of UC in the care of ORR has more than doubled since ORR began using the UC Portal in 2014—from serving 57,496 UC in 2014 to 128,904 UC in 2022.

The Unaccompanied Children Portal

The UC Portal is a web application used to collect, organize, and report data related to UC who have been referred to ORR for care until an appropriate sponsor is located who can assume custody, the UC turn 18 years old, or their immigration status is resolved. The UC Portal is a key data source for ORR reunification efforts for separated children in ORR care and contains available data on sponsors or family members and adult members of sponsoring households. It also supports interactions with other Federal Agencies and ACF management.

ORR is the primary user of the UC Portal application, which has a security categorization of moderate impact. This means that unauthorized disclosure, modification, or destruction of information contained in the UC Portal could be expected to have a serious adverse effect on ORR organizational operations, assets, or individuals. It also means that the disruption of access to or use of the UC Portal or its data could be expected to have the same serious adverse effects.

Maintenance of the application is contracted to a third-party and the hosting of the application is contracted to a cloud service provider. ACF is responsible for managing the operating system, application software, and configuration of the cloud firewall for each instance. In addition to ACF's security responsibilities for the application in the cloud environment, ACF maintains responsibility for access control, contract oversight of the application development, and contingency planning of the UC Portal application. As a result, this report is directed to ACF.

In our prior audit of the UC Portal, we made seven recommendations, as detailed in Appendix B. ACF took corrective actions to address the recommendations. As part of the current audit, we reviewed ACF's implementation of these recommendations.

System Development and Life Cycle

HHS requires use of its Enterprise Performance Life Cycle (EPLC) framework to meet National Institute of Standards and Technology (NIST) requirements related to SDLC. This EPLC applies to all HHS information technology (IT) investments and projects, including, but not limited to,

new projects; major enhancements to existing projects; projects associated with steady-state investments;[2] high-priority, fast-track IT projects; and new commercial off-the-shelf product acquisitions.

The EPLC framework organizes the activities, deliverables, and governance reviews of an IT project into 10 life-cycle phases. The EPLC framework provides a project management methodology that guides the activities of project managers, business owners, critical partners, IT governance organizations, and other stakeholders throughout the life cycle of the project to ensure an enterprise perspective is maintained during planning, execution, and governance processes. Although one of the objectives of the EPLC framework is to standardize IT project management within HHS based on best practices, the framework also allows tailoring to accommodate the specific circumstances (e.g., size, duration, complexity, and acquisition strategy) of each project.

HOW WE CONDUCTED THIS AUDIT

For 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 ACF's system security plan (SSP) for the UC Portal. 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.

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 A describes our audit scope and methodology and Appendix C contains Federal requirements related to our audit.

FINDINGS

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

[2] At the steady state, an investment is equal to depreciation, which means that all the investment is being used to repair and replace the existing capital stock.

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.

ACF IMPLEMENTED MOST OF OUR PRIOR AUDIT RECOMMENDATIONS BUT DID NOT CONSISTENTLY PERFORM USER ACCOUNT REVIEWS

ACF implemented most of our prior audit recommendations. Specifically, ACF enhanced UC data and UC Portal cybersecurity controls by (1) modifying its policies and procedures for user account management at UC care facilities,[3] (2) developing training modules for cybersecurity and "least privilege" principle, (3) modifying its policies for user account reviews, (4) finalizing its business continuity and disaster recovery plans, (5) completing functional testing of its business continuity and disaster recovery plans, (6) establishing monitoring metrics for the UC Portal application, and (7) resolving the penetration test findings.

However, ACF did not consistently perform user account reviews.[4] Its access control policy stated that user accounts are to be reviewed on a quarterly basis and accounts that have been inactive for at least 90 days are blocked and cannot be reestablished. However, we identified 30,695 inactive accounts (about 23 percent of all accounts) that were not reviewed in accordance with ACF's access control policy, including 16,772 accounts that were in inactive status for at least 1 year, which far exceeds the 90-day threshold. The following table shows the amount of time these accounts remained inactive.

Table: Inactive User Accounts by Number of Days Inactive

Days Inactive	Count of Accounts
90-179	3,526
180-269	5,073
270-364	5,324
365+	16,772
Total	**30,695**

This occurred because ACF relied on occasional reviews of a randomly, unsystematically selected number of accounts rather than quarterly reviews of all inactive accounts to determine if a user's account should be blocked. Inactive UC Portal user accounts provide opportunities for malicious actors to reactivate the accounts, falsely assume the identities of the authorized user who was assigned the account, and gain unauthorized access to UC data. ACF officials stated that they intend to implement an automated review process to ensure inactive accounts are blocked in accordance with ACF's access control policy.

[3] This recommendation was not fully implemented, the following paragraph provides additional details.

[4] The ACF access control policy for the UC Portal requires that user accounts that have not been used for 60 days have the status changed to inactive, requiring reactivation from the ACF help desk or the administrator that created the account.

ACF HAS NOT FULLY IMPLEMENTED SOME REQUIRED CYBERSECURITY CONTROLS

We determined that some required cybersecurity controls to ensure the protection of sensitive UC data in accordance with Federal requirements were not fully implemented, based on our review of ACF's SSP for the UC Portal. The SSP implements policy, assigns responsibility, and prescribes procedures for applying integrated and layered protection of the UC Portal to ensure the confidentiality, integrity, and availability of the system information. Also, ACF did not determine the implementation status of all minimum required cybersecurity controls.

The Federal Information Security Modernization Act (FISMA) of 2014 requires Federal agencies to adequately safeguard information systems and assets.[5] The security control requirements for IT systems that handle government data are documented in NIST Special Publication (SP) 800-53, Revision 4. To determine which of the security controls should be implemented to protect IT system and its data the system security categorization must be determined. The Federal Information Processing Standards 199 (FIPS Pub. 199) defines the process for determining the security categorization for IT systems and data, which may be categorized as low, moderate, or high ACF determined the security categorization for the UC Portal and data was moderate. This means that unauthorized disclosure, modification, or destruction of information contained in the UC Portal could be expected to have a serious adverse effect on ORR organizational operations, assets, or individuals. It also means that the disruption of access to or use of the UC Portal or its data could be expected to have the same serious adverse effects. In total, there are 159 NIST SP 800-53, Revision 4 controls required for systems categorized as moderate.

Our review of ACF's UC Portal SSP dated December 9, 2021, revealed that ACF documented the status of all 159 minimum required controls for a moderate system. Of the 159 controls, ACF designated 119 controls as "in place," 30 controls were in various stages of implementation,[6] and 10 controls were designated as "not applicable." Because ACF did not fully implement the 30 controls it determined were required, UC data may be at risk of unauthorized disclosure, modification or destruction and may have adverse effects on ORR operations assets and individuals. Also, the disruption of access to or the use of the UC Portal is a possibility.

ACF PERFORMED ADEQUATE SYSTEM DEVELOPMENT LIFE CYCLE PLANNING FOR THE UNACCOMPANIED CHILDREN PORTAL

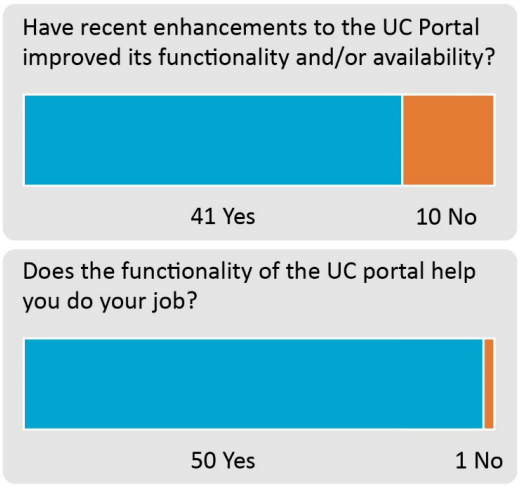
ACF established adequate SDLC planning to ensure that its current efforts to upgrade the UC Portal align with its business and performance objectives. Specifically, ACF incorporated a three-tiered governance structure that complied with the EPLC that requires and ensures the development of upgrades to the UC Portal align with its business and performance objectives.

[5] P.L. No. 113-283; enacted Dec. 18, 2014.

[6] Of the 30 controls in various stages of implementation, 2 were "not in place," 7 were "partially in place," and 20 were "planned."

The governance structure consists of two delivery teams, an executive committee, and a program committee. The two committees meet separately on a periodic basis (e.g., the program committee meets biweekly) to review input from the two delivery teams (also known as scrum teams). This collaborative effort is known as an agile scrum methodology.[7] ACF initiated this methodology in May 2022, when its UC Program Tech Delivery team held its first sprint meeting.[8] That same month, the UC Program Committee also held its first meeting.[9] ACF's Chief Technical Officer explained that, throughout the process of building the UC Portal and attempting to build a replacement for the UC Portal, the now-defunct UC Pathways System, ORR said that it learned a lot about developing a technology product to serve the needs of the UC Program.

Figure: Responses to OIG Questionnaire



To determine the level of satisfaction of UC Portal users with upgrades to the Portal, we sent a questionnaire to users at two UC intake facilities. The questionnaire focused on the functionality and availability of the UC Portal after recent upgrades. As depicted in the figure, the response to these upgrades was positive. Specifically, 41 of 51 respondents (80 percent) agreed that recent enhancements improved the functionality and/or availability of the UC Portal and 50 of the respondents (98 percent) agreed that the UC Portal helps them do their job.

[7] Agile scrum methodology is a sprint-based project management system with the goal of delivering the highest value to stakeholders. "Agile" is a process that allows a team to manage a project more efficiently by breaking it down into several stages, each of which allows for consistent collaboration with stakeholders to promote steady improvements at every stage. "Scrum" is a framework for effective collaborations among teams working on complex products. Scrum is a type of agile technology that consists of meetings, roles, and tools to help teams working on complex projects collaborate and better structure and manage their workload. https://www.businessnewsdaily.com/4987-what-is-agile-scrum-methodology.html. Accessed July 21, 2022.

[8] The UC Program Tech Delivery team does the development work, advocates for technical and infrastructure priorities, advocates for user needs, conducts research and design, and proposes prioritization of work.

[9] The UC Program Committee advocates for business and operational needs, contributes to prioritization recommendations, identifies risks and mitigation strategies, drives adoption of solutions, and celebrate success.

RECOMMENDATIONS

We recommend that the Administration for Children and Families:

- consistently perform user account reviews in accordance with its access control policy and

- fully implement the 30 required minimum controls identified in the UC Portal system security plan as being in various stages of implementation.

ACF COMMENTS AND OIG RESPONSE

In written comments, ACF concurred with two of the three recommendations in our draft report and described actions that it has taken or planned to take to implement those recommendations.

For our first recommendation, ACF stated that it has begun a single sign-on application rollout that is slated to be completed after full integration with the Department of Homeland Security's identity system.

Regarding our second recommendation, ACF stated that it has implemented 15 controls and is in process of implementing the remaining controls as it transitions to NIST 800-53, Revision 5.

Regarding the third recommendation in our draft report (to determine the status and implement, if needed, the 8 minimum required controls for which no status was documented in the UC Portal SSP and update the plan accordingly), ACF indicated that its UC Portal SSP listed all required controls and the implementation status for those controls. Based on our review of ACF's comments, including technical supporting documentation, and further analysis of ACF's UC Portal SSP, we confirmed that the 8 controls and their implementation status are listed in the UC Portal SSP. Accordingly, we removed our related finding and recommendation.

ACF's comments, excluding technical supporting documentation, are included in their entirety as Appendix D.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We assessed general IT controls and reviewed ACF's implementation of our prior audit recommendations. To accomplish this, we reviewed ACF's policies and procedures, interviewed staff, and reviewed ACF's SSP for the UC Portal. 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 upgrading the UC Portal.

We conducted our audit from November 2021 through October 2023.

METHODOLOGY

To accomplish our objective, we:

- assessed the following related to ACF UC Portal:
    - policies and procedures,
    - SSP,
    - risk assessment,
    - logical access controls,
    - EPLC procedures, and
    - information systems configuration controls,
- sent questionnaires to UC Portal users at two UC intake facilities that requested information on the users' experience with the UC Portal,
- assessed ACF's implementation of prior audit recommendations, and
- discussed with ACF officials the findings contained within this report.

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: PRIOR AUDIT RECOMMENDATIONS

We made seven recommendations in our prior audit report (*The Administration for Children and Families Did Not Adequately Implement Controls Over the Unaccompanied Alien Children Portal to Protect Sensitive Data in Accordance With Federal Requirements*, A-18-19-06002, issued December 10, 2020). Specifically, we recommended that ACF:

1. Develop and implement comprehensive access control policies and procedures that define how the UAC care facilities should assign and manage access to UAC Portal as required by NIST SP 800-53, Revision 4, for moderate impact systems.

2. Develop and conduct training of care facilities management on properly determining and assigning access privileges to users based on NIST SP 800-53, Revision 4, AC-6, for a moderate impact system to include the concept of least privilege access.

3. Develop and implement policies and procedures for user account access review in accordance with NIST SP 800-53, Revision 4, AC-6, for a moderate impact system.

4. Finalize and approve business continuity and disaster recovery plans in accordance with Federal requirements to reflect the current system environment of the UAC Portal.

5. Conduct functional testing of the business continuity and disaster recovery plans for the production system environment.

6. Develop and implement monitoring metrics for the UAC web application to monitor load on the application and alert ACF when action is needed to prevent unintended downtime.

7. Resolve the external and internal penetration test findings in accordance with the detailed recommendations for each vulnerability identified.

APPENDIX C: FEDERAL REQUIREMENTS

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

The FISMA of 2014, Public Law 113-283, section 3553, directs agencies to comply with the policies, principles, standards, and guidelines on information security promulgated under section 11331 of title 40,[10] and to coordinate the development of their information system policies and procedures in accordance with standards and guidelines submitted by the NIST under section 20 of the NIST Act (15 U.S.C. 278g-3).

15 USC 278g-3(d) includes the following:

> The Institute [NIST] shall—(1) submit standards developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Director of the Office of Management and Budget for promulgation under section 11331 of title 40; (2) provide assistance to agencies regarding—(A) compliance with the standards and guidelines developed under subsection (a) of this section; (B) detecting and handling information security incidents; and (C) information security policies, procedures, and practices.

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 199

FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems,* provides those standards for categorizing information and information systems as low-impact, moderate-impact, or high-impact for confidentiality, integrity, and availability based on security objectives. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The resulting security categorization helps the organization determine the security and privacy control baselines to protect the system, as detailed in NIST SP 800-53.

Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in NIST SP 800-53, Revision 4. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation.

[10] 40 U.S.C. § 11331 requires that Federal information systems meet the minimum information security requirements described under section 20 of the NIST Act (15 U.S.C. 278g-3).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

NIST guidance documents and recommendations are issued in the SP 800 series.[11] OMB policies (including OMB FISMA Reporting Instructions and Agency Privacy Management) state that, for other than national security programs and systems, agencies must follow NIST guidance. NIST advises:

> While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. When assessing federal agency compliance with NIST guidance, auditors, evaluators, and assessors should consider the intent of the security concepts and principles articulated within the guidance document and how the agency applied the guidance in the context of its specific mission responsibilities operational environments, and unique organizational conditions.

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

> provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors (both intentional and unintentional).

NIST SP 800-160, Volume 1, *Systems Security Engineering*: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems:

> The principles for secure evolution of the system design address changes driven by the natural evolution of the system as planned; by changes in stakeholder objectives and concerns; by technology obsolescence; or by changes in the nature of disruptions, hazards, and threats and the effectiveness of system protection. These types of changes require periodic assessment of the concept of secure function; architecture, viewpoints, and the validity of the prevailing viewpoints; and the assumptions, forecasts, inferences, correspondence, and constraints associated with all of the above.

[11] The NIST SP 800 Series is available online at http://csrc.nist.gov/publications/PubsSPs.html.

APPENDIX D: ACF COMMENTS

ADMINISTRATION FOR CHILDREN & FAMILIES

Office of the Assistant Secretary | 330 C Street, S.W., Suite 4034
Washington, D.C. 20201 | www.acf.hhs.gov

February 15, 2024

Ms. Amy Frontz
Deputy Inspector General for Audit Services
U.S. Department of Health and Human Services
330 Independence Avenue, SW
Washington, DC 20201

Dear Ms. Frontz:

The Administration for Children and Families (ACF) appreciates the opportunity to respond to the Office of Inspector General's (OIG) draft report, *ACF Has Enhanced Some Cybersecurity Controls Over the Unaccompanied Children (UC) Portal and Data But Improvements Are Needed* (A-18-22-03200). Please find our comments and responses to the draft report recommendations below.

Recommendation 1: We recommend that ACF consistently perform user account reviews in accordance with its access control policy.

Response: ACF concurs with this recommendation.

ACF has undertaken efforts to ensure that user account reviews are consistently being conducted in accordance with ACF's Access Control (AC) Policy and the ORR User Management Plan (UMP) developed in 2020, which further expands on ACF's AC policy requirements. The immediate implementation of the UMP resulted in a mass account clean-up conducted from June through August of 2022 to remove all inactive accounts and develop a UC Portal Account Request Form and approval processes.

To better manage users, sustain effective day-to-day management, and enforce the UMP consistently through technical controls, beginning in early 2022, ACF developed a single sign-on tool for all Office of Refugee Resettlement (ORR) systems, the App Launcher, which allows for role-based management of user access and entitlements. User access to App Launcher (and thereby other UC Program applications) for contractor and grantee field staff is managed by site admins, who, by policy, are responsible for managing their staff access and who have better and more timely knowledge of hires and resignations at their site than ACF could achieve centrally. The App Launcher enforces the requirements for cybersecurity and rules of behavior training by granting any user access until the system uploads and confirms certificates of completion. While site admins are held accountable for timely revocation of access for their staff, App Launcher includes timer-based expiration of user access and audit tools for detecting whether a user has been active or inactive for a set number of days. It enables ACF staff to reach out to site admins when anomalies appear. After 30 days of inactivity, the accounts are automatically frozen, and an admin must take action to unfreeze the account should it need to be reinstated. Access gets

revoked after 60 days of inactivity, and the account is set to inactive status. Pilot users began using App Launcher in April of 2022, with expansion to all ORR staff, contractors, and grantees completed by October 2023. Implementation of App Launcher will be complete, with no access to UC Portal allowed other than through App Launcher, following the final phase of building integration with the Department of Homeland Security's identity system. This is anticipated by the end of Spring 2024.

Recommendation 2: We recommend that ACF fully implement the 29 required minimum controls identified in the UC Portal system security plan as being in various stages of implementation.

Response: ACF concurs with this recommendation.

ACF's UC Portal system security plan (SSP) has been updated since the OIG's audit period. The new SSP, effectuated on November 24, 2023, has improved the control implementation identified in this recommendation. Since the audit period, 15 security controls (AC-1, AT-3, AT-4, AU-6, AU-7, AU-11, AU-12, CA-7, CP-2, CP-3, CP-4, IA-5, IR-1, PL-8, and SI-2) have been fully implemented, while the remaining 14 security controls (AU-1 CA-1, CM-1, CP-1, IA-1, MA-1, MP-1, PE-1, PL-1 PS-1, RA-1, SA-1, SC-1, and SI-1) have progressed to the planned stage. ACF plans to remediate these remaining controls as it continues to adopt NIST 800-53 Revision 5 into its systems environments by the end of calendar year 2024.

Recommendation 3: We recommend that ACF determine the status and implement, if needed, the 8 minimum required controls for which no status was documented in the UC Portal system security plan and update the plan accordingly.

Response: ACF does not concur with this recommendation.

As of December 9, 2021, the eight minimum required controls referenced by OIG were listed, and their implementation status was documented, in the Appendix of the SSP. In every iteration of the SSP revisions, the controls have been listed with an implementation status in an SSP Appendix X.

Again, we appreciate the opportunity to review and comment on this draft report. Please direct any follow-up inquiries on this response to Corbin Kenaley, Office of Legislative Affairs and Budget, at (202) 536-8955.

Sincerely,

Jeff Hild
Acting Assistant Secretary
Administration for Children and Families
U.S. Department of Health and Human Services