Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

ADMINISTRATION FOR CHILDREN AND FAMILIES DATA HOSTED IN CERTAIN CLOUD INFORMATION SYSTEMS MAY BE AT A HIGH RISK OF COMPROMISE

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-18-22-08020

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-18-22-08020

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

Administration for Children and Families Data Hosted in Certain Cloud Information Systems May Be at a High Risk of Compromise

Why OIG Did This Audit

This audit is one in a series of audits that will examine whether HHS and its Operating Divisions have implemented effective cybersecurity controls for cloud information systems in accordance with Federal security requirements and guidelines.

Our objectives were to determine whether the Administration for Children and Families (ACF) (1) accurately identified and inventoried its cloud computing components and (2) implemented security controls in accordance with Federal requirements and guidelines.

How OIG Did This Audit

We reviewed ACF's cloud inventory and its policies and procedures. We also analyzed the configuration settings of ACF vulnerability scanners. We performed external, internal, and web application penetration testing of selected cloud information systems from April through May 2022. We also conducted two simulated phishing campaigns that included a limited number of ACF personnel during this period. We contracted with Breakpoint Labs, LLC (BPL), to conduct the penetration test on OIG's behalf. We closely oversaw the work performed by BPL, and the assessment was performed in accordance with agreed upon Rules of Engagement.

What OIG Found

ACF did not accurately identify and inventory all of its cloud computing assets. Also, although ACF had implemented some security controls to protect its cloud information systems, it did not effectively implement several other security controls to protect its cloud information systems in accordance with Federal requirements and guidelines. This occurred because ACF did not establish policies and procedures to inventory and monitor cloud information system components. Also, ACF did not perform adequate cloud and web application technical testing techniques against its systems to proactively identify the vulnerabilities we discovered. As a result, ACF data hosted in certain systems may potentially be at a high risk of compromise.

What OIG Recommends and ACF Comments

We made a series of recommendations to ACF to improve its security controls over cloud information systems, including that it update and maintain a complete and accurate inventory, remediate the 19 security control findings identified in our report, and leverage cloud security assessment tools to identify misconfigurations and weak cybersecurity controls in its cloud infrastructure.

In written comments on our draft report, ACF concurred with our recommendations and described the actions it has taken or plans to take to address them, including (1) tracking its inventory in a new Governance, Risk, and Compliance system; (2) crafting steps for staff to effectively implement cloud security baselines; and (3) leveraging HHS Department-level penetration testing services to give ACF real-time visibility into exploitable vulnerabilities across a variety of assets. Although we have not yet confirmed whether ACF effectively implemented our recommendations, we are encouraged by ACF's response and we look forward to receiving and reviewing the supporting documentation through our audit resolution process.

The full report can be found on the OIG website.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

In June 2019, the Office of Management and Budget published its updated *Federal Cloud Computing Strategy* to accelerate information technology (IT) modernization through agency adoption of cloud-based solutions. Since then, Federal agencies are increasingly adopting cloud services to address their IT needs and potentially save money and time to meet their critical missions. In 2022, the Department of Health and Human Services (HHS) reported that more than 30 percent of its 1,555 systems were cloud-based.

Federal agencies are required to protect Federal information processed or stored in cloud information systems to ensure the confidentiality, integrity, and availability of the information. Considering the potential wide-scale impact that a successful cyberattack against cloud information systems may have across HHS, we are performing a series of audits that will examine whether HHS and its Operating Divisions (OpDivs) have implemented effective cybersecurity controls for cloud information systems owned, operated, or maintained by HHS or its contractors in accordance with HHS policy and Federal requirements and guidelines.[1, 2]

We conducted this audit to determine whether the Administration for Children and Families (ACF) is securing its cloud computing components in accordance with HHS policies and Federal requirements, including security controls outlined by the National Institute of Standards and Technology (NIST).[3]

OBJECTIVES

Our objectives were to determine whether ACF (1) accurately identified and inventoried its cloud computing components and (2) implemented security controls in accordance with Federal requirements and guidelines.

[1] An information system is defined by the National Institute of Standards and Technology as "A discrete set of information components organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

[2] These audits will assess the security of cloud information system configurations and include tests to detect any attack vectors that adversaries could leverage to access, alter, destroy, or exfiltrate data within cloud information systems or disrupt operations. The results from these audits will allow us to identify cybersecurity risks in cloud-based information systems that have not yet been identified, remediated, or both.

[3] Cloud computing components include networks, servers, storage, applications, services, etc. NIST Special Publication (SP) 800-145. Available online at https://csrc.nist.gov/publications/detail/sp/800-145/final. Accessed on Oct. 24, 2023. NIST SP 800-53. Available online at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Accessed on Oct. 24, 2023.

BACKGROUND

Administration for Children and Families

ACF's mission is to foster health and well-being by providing Federal leadership, partnership, and resources for the compassionate and effective delivery of human services. ACF program offices are specialized to support a variety of initiatives that are intended to empower families and individuals and improve access to services to create strong, healthy communities. These programs fund a variety of projects, including Native American language preservation, refugee resettlement and childcare.

Cloud Computing

NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable virtualized computing components (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction by an organization.[4] The cloud computing model is composed of the following three service models:

- Infrastructure-as-a-Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing components where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

- Platform-as-a-Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

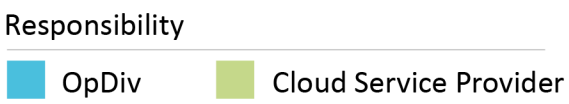
- Software-as-a-Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

As displayed in Table 1 (following page), each service model involves different shared security responsibilities between the organization and the cloud service provider. Our audit focused on ACF's security responsibilities.

[4] NIST definitions of cloud computing terms in this report are contained in NIST Special Publication (SP) 800-145, "The NIST Definition of Cloud Computing." Available online at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Accessed on Nov. 28, 2023.

Table 1: Cloud Computing Security Responsibilities

IaaS Security	PaaS Security	SaaS Security
Data	Data	Data
Application	Application	Application
Platform	Platform	Platform
Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical



ACF leverages these cloud service models to process, store, or transmit certain ACF mission-related information. During our audit, approximately 62 percent of ACF's information systems were hosted by cloud service providers.

With significant increases in cyberattacks against the Federal Government, such as email phishing and privilege escalation, ACF cloud information systems are potential targets for hackers.[5] ACF cloud information systems host sensitive data pertaining to families and individuals, communities, and programs, which is the type of information sought by malicious adversaries. This data, if compromised, may be used by adversaries to engage in child exploitation, or to sabotage the confidentiality, integrity, and availability of the ACF data hosted within cloud information systems.

HOW WE CONDUCTED THIS AUDIT

For our audit, we selected and examined certain security controls for which ACF is responsible for implementing. The scope of the audit included all cloud information systems owned, operated, or maintained by ACF or its contractors. We reviewed ACF's cloud systems inventory and its policies and procedures. We also assessed the configuration settings of an ACF cloud environment using a cloud security assessment tool. Also, we performed penetration testing of selected cloud information systems in April and May 2022 to determine whether the controls in place would prevent cyberattacks.[6] Our penetration test included a focus on public IP

[5] A privilege escalation attack is a cyberattack designed to gain unauthorized privileged access into a system.

[6] Penetration tests are intended to identify vulnerabilities and security flaws in systems, devices, and controls that are in place to protect customer information and components. This type of information security testing typically attempts to simulate attacks that are either internal to an organization's computer network (i.e., from employees or hired contractors) or outside an organization's network boundary (e.g., State sponsors and organized crime).

addresses and domain names owned and operated by ACF or ACF contractors. We specified the systems that were to be tested within the Rules of Engagement (RoE) signed by the Office of the Inspector General (OIG), an OIG contractor, and ACF.

To assist us with this audit, we relied on the work of specialists. Specifically, we contracted with Breakpoint Labs, LLC (BPL), to conduct the penetration test of ACF systems. BPL provided subject matter expertise throughout the assessment of ACF's cloud information systems. To simulate a real-world attack more closely, the penetration testing team was given no substantial information before the testing began. This scenario is known as a zero-knowledge, or Black Box, penetration test. The penetration testing team also completed two different email phishing campaigns during the audit period. We performed testing in accordance with the agreed-upon RoE document. We provided detailed documentation about our preliminary findings to ACF in advance of issuing our draft 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 A contains the details of our audit scope and methodology, Appendix B describes the tools we used to conduct the audit, and Appendix C contains the Federal requirements.

FINDINGS

ACF did not accurately identify and inventory all of its cloud computing components. Also, although ACF implemented some security controls to protect its cloud information systems, it did not effectively implement several other security controls to protect its cloud information systems in accordance with Federal requirements and guidelines. As a result, ACF data stored in certain cloud information systems may potentially be at a high risk of compromise.

ACF INVENTORY OF ITS CLOUD COMPUTING COMPONENTS WAS INACCURATE

NIST SP 800-53, Revision 4, requires organizations to develop and document an inventory of information system components that (1) accurately reflects the current information system; (2) includes all components within the authorization boundary of the information system; and (3) is at the level of granularity deemed necessary for tracking and reporting. However, ACF's inventory of its cloud computing components was inaccurate. Specifically, we identified three cloud-hosted websites through our penetration testing that were not documented in ACF's inventory. We notified ACF of the additional assets identified, and ACF concurred that the assets were part of its enterprise and should have been included in the inventory.[7]

[7] During our testing, we informed ACF of any newly discovered assets and added them to the RoE.

ACF's inventory was inaccurate because it did not establish policies and procedures to inventory and monitor cloud information system components. If ACF does not accurately inventory its components, it may overlook implementing the controls to adequately secure them. As a result, out-of-date, misconfigured, or unpatched websites that are susceptible to a cyberattack may exist unbeknownst to ACF in its computing environment. This could lead to unauthorized modifications and execution of systems commands to compromise sensitive data, including personally identifiable information such as unaccompanied children's records. In addition, the ability to detect a threat or indicator of compromise from those components may be limited, potentially allowing a bad actor to gain a foothold on the network and compromise or attack other components.

SOME ACF CLOUD INFORMATION SYSTEM SECURITY CONTROLS WERE NOT EFFECTIVE

Although we found some system controls to be effective at preventing our email phishing attacks and simulated cyberattacks against internet-facing systems we tested, several security controls were not effective in preventing other types of simulated cyberattacks. Overall, we found 19 security controls for ACF cloud information systems that need to be improved to comply with Federal requirements. During our testing, we were able to exploit certain vulnerabilities to gain additional system privileges to access sensitive data and obtain unauthorized control of cloud components. The most critical findings were related to unintended exposure of sensitive information and a lack of effective input validation on public web sites.[8] Table 2 lists the NIST SP 800-53, Revision 4, security control findings that we identified. The findings are ordered by risk rating, as determined by OIG.

Table 2: ACF Cloud Information Security Control Findings

NIST SP 800-53, Revision 4, Security Control	Control No.*	Security Control Finding	Risk Rating
Access Enforcement	AC-3	ACF did not prevent unauthorized exposure of sensitive information within 11 cloud components.	Critical
Information Input Validation	SI-10	ACF did not adequately sanitize or verify information system input for two public-facing web applications hosted in the cloud.	Critical
Device Lock	AC-11	For seven cloud components, ACF did not implement session lock controls that terminated access after a defined period of inactivity on the components.	High

[8] Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering malfunction of various downstream components. Available online at https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html. Accessed on Oct. 24, 2023.

NIST SP 800-53, Revision 4, Security Control	Control No.*	Security Control Finding	Risk Rating
Least Privilege	AC-6	ACF did not configure access control policies for eight cloud components to ensure authorized users were granted the minimum rights needed to perform their duties.	High
Policies and Procedures	CA-1	ACF did not adequately enforce organizational and system-level policies and procedures to address cloud security compliance with Federal regulations.	High
Audit Record Review, Analysis, & Reporting	AU-6	ACF did not enforce the review and analysis of system audit records for indications of inappropriate or unusual activity within seven cloud components.	High
Baseline Configuration	CM-2	ACF did not implement secure baseline configuration controls for one cloud component.	High
Least Functionality	CM-7	ACF did not effectively enforce least functionality controls on five cloud components.	High
User-Installed Software	CM-11	ACF did not adequately enforce policies governing the installation of user-installed software on five cloud components.	High
Flaw Remediation	SI-2	ACF did not install security-relevant software updates in 11 cloud components in a timely manner.	High
Identification & Authentication (Organizational Users)	IA-2	ACF did not implement multifactor authentication for network access within its cloud information system for five privileged accounts. In addition, ACF did not enforce password authentication on seven cloud components.	High
Authenticator Management	IA-5	ACF did not enforce NIST password complexity requirements on six cloud components.	High
Account Management	AC-2(1), AC-2(4)	ACF did not employ automated controls to ensure access key rotation for over 30 cloud components and user accounts.	Medium

NIST SP 800-53, Revision 4, Security Control	Control No.*	Security Control Finding	Risk Rating
Unsuccessful Logon Attempts	AC-7	ACF did not configure four web application portals hosted in the cloud to limit the number of invalid logon attempts by a user.	Medium
Transmission Confidentiality and Integrity	SC-8	ACF did not enforce web traffic encryption on two websites.	Medium
Authorization	CA-6	ACF did not provide evidence of security assessment and authorization documentation for four cloud information systems.	Medium
Protection of Information at Rest	SC-28	ACF did not enforce native cryptographic mechanisms to protect the confidentiality and integrity of cloud data logs. It also did not enforce cryptographic protection for 534 cloud storage components to prevent unauthorized disclosure and modification of data.	Medium
System Security Plan	PL-2	ACF did not update its system security plans for 11 cloud information systems in accordance with Federal requirements.	Low
Malicious Code Protection	SI-3	ACF did not adequately employ malicious code protections for a web application to detect and prevent malicious code attacks.	Low

* The Control No. is the abbreviation of the control family name and the number of the specific control within NIST SP 800-53, Revision 4. All controls within this table are applicable within NIST SP 800-53, Revision 5.

The security control findings that we identified occurred because ACF's cloud security procedures did not outline specific steps that system administrators should follow to effectively implement cloud security baselines, and secure cloud components in accordance with HHS requirements. The control findings also were not detected or detected timely because ACF did not perform adequate cloud and web application technical testing techniques to proactively identify the vulnerabilities.

Failure to properly implement these required security controls places certain ACF cloud information systems at a potentially higher risk of malicious attacks by bad actors. The weak security controls may be exploited by adversaries who seek to steal or distort sensitive data, and disrupt operations, the ACF cloud infrastructure, or both. One technique used by adversaries is resource hijacking. Adversaries typically use this technique against cloud

information systems that are not properly configured. According to the CrowdStrike 2023 Global Threat Report, resource hijacking was identified as the most common technique used by adversaries in 2022. The technique is "destructive, with actors removing access to accounts, terminating services, and destroying data and deleting components."[9] Its effect would be a possible loss of system confidentiality, integrity, and availability, leading to a potential loss of public trust in ACF programs.

RECOMMENDATIONS

We recommend that the Administration for Children and Families:

- update and maintain a complete and accurate inventory of information systems hosted in the cloud,
- remediate the 19 security control findings in accordance with NIST SP 800-53,
- update its cloud security procedures to include detailed steps for operational staff to effectively implement cloud security baselines in accordance with HHS requirements,
- leverage cloud security assessment tools to identify misconfigurations and weak cybersecurity controls in its cloud infrastructure, and
- conduct testing of its cloud information systems that includes the emulation of an adversary's tactics and techniques on a defined reoccurring basis.

ACF COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments on our draft report, ACF concurred with our recommendations and described actions it has taken or plans to take to address them. A summary of ACF's comments and our responses follows. ACF's comments are included in their entirety as Appendix D.

Regarding our first recommendation, ACF stated that it is in the process of transitioning its inventory of information systems to a new Governance, Risk, and Compliance system that it expects to be completed by October 2024. ACF also stated that it has implemented an automated process for discovering assets and has tagged all assets to identify their purpose and ownership.

Regarding our second recommendation, ACF indicated that it has completed a security control assessment of at least 60 percent of its FISMA systems and expects to complete assessments of the remaining systems and transition them to NIST 800-53, Revision 5 by 2025.

[9] CrowdStrike 2023 Global Threat Report p.15. Available online at https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf. Accessed on Oct. 24, 2023.

Concerning our third recommendation, ACF affirmed that it has crafted detailed steps for its IT Operations staff to effectivity implement cloud security baselines and, since May 2022, has been provisioning new servers with Defense Information Systems Agency security technical implementation guides or Center for Internet Security benchmarks.

In response to our fourth recommendation, ACF indicated that, in October 2022, it procured several products that will aid in detecting misconfigurations in cloud assets, as well as endpoint detection and response, code scanning, and file integrity assessment tools.

In response to our fifth recommendation, ACF stated that, since May 2022, it has leveraged HHS Department-level penetration testing services intended to give ACF's security team real time visibility into exploitable vulnerabilities across a variety of assets.

Although we have not yet confirmed whether ACF effectively implemented our recommendations, we are encouraged by ACF's comments and timely response. We look forward to receiving and reviewing the supporting documentation through our audit resolution process.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

The scope of this audit was all cloud information systems identified in the agreed-upon RoE document. We included any additional cloud information systems we discovered during our testing to the audit scope. We focused the penetration test on public IP addresses and domain names, web applications, and cloud information systems owned or operated by ACF or its contractors. We audited the security controls for which ACF or its contractors are responsible and did not audit the underlying infrastructure security controls that the cloud service provider is responsible for managing.

We performed our work remotely. Testing began April 5, 2022, and concluded May 2, 2022. In addition, the penetration testing team completed two phishing campaigns between April 20 and April 29, 2022. Our first campaign targeted 45 ACF cloud users. The second campaign targeted 38 ACF employees.

METHODOLOGY

We reviewed ACF policies and procedures related to the inventory of cloud information systems and assessed whether required systems controls were in place and operating effectively in accordance with NIST SP 800-53, Revision 4. We relied on the work of specialists to assist with the series of OIG audits utilizing network and web application penetration testing and social-engineering techniques. OAS contracted with BPL to conduct the penetration test of the ACF cloud information system. BPL provided subject matter experts who conducted the penetration test of all systems identified in the RoE document. In addition, BPL planned and executed two simulated email phishing campaigns against a subset of the ACF cloud users. OAS oversaw the work to ensure that all objectives were met, and testing was performed in accordance with generally accepted government auditing standards and the RoE document.

Our testing focused on the cloud information systems or infrastructure used to support ACF applications and operations. It included web application penetration testing to assess the effectiveness of security controls for targeted web applications. In addition, it included testing the ACF Amazon Web Services (AWS) cloud information system from a Black Box and Gray Box perspective, along with two social engineering campaigns we launched within the testing timeline.[10, 11]

[10] AWS is a bundled remote computing service that provides cloud computing infrastructure over the Internet with storage, bandwidth, and customized support for application programming interfaces.

[11] Black Box Testing is a test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Gray Box Testing is a test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object.

To accomplish our objectives, OIG and ACF prepared the RoE document that outlined the general rules, logistics, and expectations for the penetration test.

In April 2022, we began reconnaissance and scope verification of cloud components owned, operated, and maintained by ACF. We then performed cloud penetration testing to determine whether internet-facing cloud information systems were susceptible to exploits by an external attacker. We also tested to identify gaps in ACF's cloud defense mechanisms, cloud component configurations, and data exfiltration prevention and detection controls.

The penetration testing team performed procedures and testing activities specified in Table 3:

Table 3: Penetration Testing Methodology

Infrastructure Testing	Description	Tools or Methods
Enumeration	Activity aimed at identifying devices and components within the customer network and cross-referencing with provided inventory lists.	Testers utilized automated reconnaissance scanners and other analysis tools.
Vulnerability Assessment	Perform network-based vulnerability assessment of servers, workstations, and any other network device or appliance included in our scope. The assessment identifies vulnerabilities associated with network services, operating systems, and software.	Testers utilized automated vulnerability scanners and other analysis tools.
Penetration Testing	Attempt to exploit vulnerabilities identified from vulnerability scanning to determine the extent of the vulnerability and potential remediation steps that may be taken.	Testers utilized penetration testing tools and manual techniques.

Web application penetration testing assesses the effectiveness of security controls of target web applications. The tests we performed were intended to find errors in the source code, produce unintended responses from the application, and identify any flaws in the application that can be used to exploit vulnerabilities identified because of the weak controls. Table 4 (next page) describes our web application testing techniques.

Table 4: Web Application Testing Techniques

Web Application Test Techniques	Description
Visible Code Review	Reviewed the available source of pages to identify code and/or comments that may provide useful information, hidden form variables, and directory names.
Role Function Testing or Role-Based Access Control	Verified that role-based access controls properly restrict or provide access to data within the application as defined by the business logic.
Error Handling	Analyzed error, debug, and exception messages originated from the web server or database that may reveal any information that may be useful to an attacker.
Forceful Browsing / Directory Brute Forcing	Attempted to discover directories and files by appending known or standard names to the URL. Based on information gathered, attempted to find sensitive information, debug, or log files.
Administration Interfaces	Attempted to locate known administration interfaces based on known information, and manually enter the directory and port of default administrative sites. Exploitation of the manufacturer default credentials, common credentials, and previously discovered credentials all may be attempted when testing these interfaces.
Parameter Tampering	Attempted parameter tampering, which is a technique that takes advantage of a lack of input validation on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL). Modifications to these parameters can be used to bypass the security mechanisms of the application.
SQL Injection	Attempted SQL injection, which is a technique used to take advantage of a lack of input validation on user-submitted data that are passed from the web application to a backend database. The user-submitted data are then executed by the database and can be used to bypass authentication or gain access to unauthorized information.
Session Management/Hijacking	Attempted session hijacking, which is a technique used to take control of a user's session after obtaining the authentication ID. The authentication ID can be obtained by brute force, reverse engineering, or captured through methods such as cross-site scripting (XSS). Once the authentication ID is obtained, a user's session can be hijacked.
Cross-Site Request Forgery (CSRF or XSRF)	Attempted CSRF, which is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

Web Application Test Techniques	Description
Cross-Site Scripting (XSS)	Attempted XSS, which is a common vulnerability discovered in web applications, enables attackers to inject client-side scripts into web application pages that are processed by the server. XSS vulnerabilities vary in risk depending on the circumstances under which the vulnerability can be exploited and the presence of the exploits.
Directory Traversal	Attempted directory traversal (or path traversal), which is when vulnerabilities can be the result of poor security validation, sanitization, or both, of user-supplied inputs. Successful exploitation may allow the attacker to determine, read, or edit files and file structures on the remote server.
Command Injection	Attempted malicious code injection, which can be the result of poorly configured or coded applications. It can be used to run operating system commands on a vulnerable server, which can lead to a complete compromise of confidentiality, integrity, and availability.

In April 2022, BPL conducted two different simulated phishing campaigns to determine whether ACF implemented appropriate controls to detect and prevent successful phishing campaigns and to determine whether ACF personnel were adequately trained to recognize and appropriately respond to such malicious emails. ACF provided OIG a list of employees and contractors that have access to the ACF cloud environments and applications to perform their duties. Under direction from the OIG, these employees and contractors were subject to BPL's simulated phishing campaign. The first campaign was designed to gather information about the user's browser and computer OS, which could then be used as reconnaissance. The second campaign was designed for users to open emails and click on a link to a webpage to download a utility zip file containing our malicious executable.

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 meets the required standards based on our audit objectives.

APPENDIX B: TOOLS WE USED TO CONDUCT THE AUDIT

Droopescan

Droopescan is a plugin-based scanner that is used to identify any issues in Drupal-based content management systems. Droopescan is similar to network scanners like Network Mapper (Nmap) but is used to scan Drupal-based systems instead. Drupal is an open-source content management framework and is often used to manage and administer websites. Droopescan is often used to spot bugs and issues with the Drupal script and can potentially be used to highlight any exploitable issues.

Nmap

Nmap is a free and open-source utility for network discovery and security auditing. Nmap is also utilized by penetration testers to obtain network inventory, manage service upgrade schedules, and monitor host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters or firewalls are in use, and dozens of other characteristics.

Pacu

Pacu is an open-source AWS exploitation framework, designed for offensive security testing against cloud information systems. Created and maintained by Rhino Security Labs, Pacu allows penetration testers to exploit configuration flaws within an AWS account, using modules to easily expand its functionality. Current modules enable a range of attacks, including user privilege escalation, backdooring of Identity and Access Management users, attacking vulnerable AWS Lambda functions, and much more.[12]

CloudMapper

CloudMapper is an open-source AWS cloud visualization tool used to analyze AWS cloud information systems. CloudMapper generates interactive network diagrams of AWS accounts, allowing penetration testers to understand AWS cloud information systems included in the audit scope.

Scout Suite

Scout Suite is an open-source, multi-cloud security-auditing tool that enables security posture assessment of cloud information systems. Using the Application Programming Interfaces (APIs) exposed by cloud providers, Scout Suite gathers configuration data for manual inspection and

[12] AWS Lambda is a serverless, event-driven computer service that lets a person run code for virtually any type of application or backend service without provisioning or managing servers.

highlights risk areas.[13] Scout Suite was designed by security consultants/auditors. It is meant to provide a point-in-time, security-oriented view of the cloud account it was run in. Once the data has been gathered, all analysis can be performed offline.

Nessus

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language, a simple language that describes individual threats and potential attacks.

Shodan

Shodan is a search engine that allows users to search for various types of servers (webcams, routers, etc.) connected to the Internet using a variety of filters. Shodan provides information about the server software, what options the service supports, a welcome message, or anything else that the client can find out before interacting with the server.

Censys.io

Censys.io is a web-based search platform for assessing an attack surface for Internet connected devices. The tool can be used not only to identify Internet-connected components and Internet of Things/Industrial Internet of Things but also Internet-connected industrial control systems and platforms.

Domain Dossier

The Domain Dossier tool generates reports from public records about domain names and IP addresses to help solve problems, investigate cybercrime, or just better understand how things are configured. These reports include the owner's contact information, registrar information, and registry information.

[13] An API is a set of defined rules that enable different applications to communicate with each other.

APPENDIX C: HHS AND FEDERAL REQUIREMENTS

FEDERAL REGULATIONS

DHS Cybersecurity and Infrastructure Agency (CISA) Binding Operational Directive (BOD) 18-01, requires federal agencies to:

> Ensure all publicly accessible Federal websites and web services provide service through a secure connection (HTTPS-only, with HSTS).

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

> AC-2(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT (page 20)
>
> Control:
> a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
> b. Assign account managers;
> c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;
> d. Specify:
> 1. Authorized users of the system;
> 2. Group and role membership; and
> 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;
> e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;
> f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];
> g. Monitor the use of accounts;
> h. Notify account managers and [Assignment: organization-defined personnel or roles] within:
> 1. [Assignment: organization-defined time period] when accounts are no longer required;
> 2. [Assignment: organization-defined time period] when users are terminated or transferred; and
> 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;
> i. Authorize access to the system based on:
> 1. A valid access authorization;

2. Intended system usage; and
3. [Assignment: organization-defined attributes (as required)];

j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

AC-2(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS (page 21)

Control:
Automatically audit account creation, modification, enabling, disabling, and removal actions.

Discussion:
Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

AC-3 ACCESS ENFORCEMENT (page 23)

Control:
Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Discussion:
Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS (page 39)

Control:

a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action] when the maximum number of unsuccessful attempts is exceeded.

AC-11 DEVICE LOCK (page 42)

Control:

a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; and
b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

CA-1 POLICY AND PROCEDURES (page 83)

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
    1. [Selection (one or more): organization-level; mission/business process-level; system level] audit and accountability policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
c. Review and update the current audit and accountability:
    1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
    2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING (page 70)

Control:

a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;
b. Report findings to [Assignment: organization-defined personnel or roles]; and
c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

CM-2 BASELINE CONFIGURATION (page 97)

Control:

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
b. Review and update the baseline configuration of the system:
    1. [Assignment: organization-defined frequency];
    2. When required due to [Assignment organization-defined circumstances]; and
    3. When system components are installed or upgraded.

CM-7 LEAST FUNCTIONALITY (page 104)

Control:

a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and
b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].

IA-2 IDENTIFICATION AND AUTHENTICATION (page 131)

Control:

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

CM-11 USER-INSTALLED SOFTWARE (page 112)

Control:

a. Establish [Assignment: organization-defined policies] governing the installation of software by users;
b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and

c. Monitor policy compliance [Assignment: organization-defined frequency].

CA-6 AUTHORIZATION (Page 89)

Control:

a. Assign a senior official as the authorizing official for the system;
b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
c. Ensure that the authorizing official for the system, before commencing operations:
    1. Accepts the use of common controls inherited by the system; and
    2. Authorizes the system to operate;
d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
e. Update the authorizations [Assignment: organization-defined frequency].

PL-2 SYSTEM SECURITY AND PRIVACY PLANS (page 214)

Control:

a. Develop security and privacy plans for the system that:
    1. Are consistent with the organization's enterprise architecture;
    2. Explicitly define the constituent system components;
    3. Describe the operational context of the system in terms of mission and business processes;
    4. Identify the individuals that fulfill system roles and responsibilities;
    5. Identify the information types processed, stored, and transmitted by the system;
    6. Provide the security categorization of the system, including supporting rationale;
    7. Describe any specific threats to the system that are of concern to the organization;
    8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];
c. Review the plans [Assignment: organization-defined frequency];
d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
e. Protect the plans from unauthorized disclosure and modification.

IA-5 AUTHENTICATOR MANAGEMENT (page 138)

Control:
Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts changes.

AC-6 LEAST PRIVILEGE (page 36)

Control:
Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion:
Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems. The principle that a security architecture is designed so that each entity is granted the minimum system components and authorizations that the entity needs to perform its function.

SC-28 PROTECTION OF INFORMATION AT REST (page 316)

Control:

Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY (page 304)

Control:
Protect the [Assignment (one or more): confidentiality, integrity] of transmitted information.

SI-2 FLAW REMEDIATION (page 333)

Control:

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within [Assignment: organization defined time period] of the release of the updates; and
d. Incorporate flaw remediation into the organizational configuration management process.

SI-3 MALICIOUS CODE PROTECTION (page 334)

Control:

a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
c. Configure malicious code protection mechanisms to:
    a. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and
    b. [Selection (one or more): block malicious code; quarantine malicious code]; take [Assignment: organization-defined action]; and send alert to [Assignment: organization defined personnel or roles] in response to malicious code detection; and
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-10 Information Input Validation (page 349)

Control:
Check the validity of the following information inputs: [Assignment: organization defined information inputs to the system].

HHS REQUIREMENTS

HHS Policy for Information Security and Privacy Protection (IS2P)

HHS Minimum Security Configuration Guidance

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 (OIG) draft report, *Administration for Children and Families Data Hosted in Certain Cloud Information Systems May Be at a High Risk of Compromise* (A-18-22-08020). Please find our comments and response to the draft report recommendations below.

Recommendation 1:
We recommend that ACF update and maintain a complete and accurate inventory of information systems hosted in the cloud.

Response: ACF concurs with this recommendation.

Since 2021, ACF has made a concerted effort to invest in the cybersecurity resources necessary to enhance its portfolio of federal information systems. ACF currently keeps and maintains comprehensive inventory of all systems that is regularly updated. This includes the collection of websites, host names, data center location, information technology (IT) investment information, federal and contractor support staff information, and software and hardware data. As of May 2023, ACF begun the effort of transitioning from maintaining its inventory via spreadsheets to leveraging its Governance, Risk and Compliance System. The transition is expected to be completed by the end of fiscal year (FY) 2024. Further, as of June 2023, ACF has implemented improvements to its IT governance process, including Federal Information Technology Acquisition Reform Act reviews, to ensure information systems are being identified prior to acquisition or development.

Throughout Summer 2023, new management of ACF's Office of Chief Information Officer (OCIO) began an extensive program of changes to cloud and application management to aggressively improve control and tracking of information systems hosted in its cloud environments. These changes included tools for automating the management and monitoring of information systems. First, management executed a broad scale assessment of the cloud environments and launched a process of consolidation and cleanup of issues such as orphaned servers and repositories of snapshots. Based on discoveries made during that process, as of October 2023, ACF is now implementing automation for asset discovery and management.

Furthermore, as a result of these efforts, all assets within the infrastructure have been tagged and now identify the purpose of the asset and the system each asset supports. The tagging effort was an additional corrective measure for improving the accuracy of our system inventory. Tagging has enabled granular automated reporting via cloud service provider tools and will enable automated asset discovery and management through implementation of other third-party tools, which is currently in process.

Recommendation 2:
We recommend that ACF remediate the 19 security control findings in accordance with NIST SP 800-53.

Response: ACF concurs with this recommendation.

ACF is transitioning all information systems to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, security controls instead of the Revision 4 security controls that were being assessed during the audit period. Security control assessments are conducted to ensure the appropriate subset of security controls have been applied and implemented. These assessments have been applied to 58 of ACF's 97 (60 percent) authorized information systems. The remaining 39 information systems are actively being upgraded to Revision 5. ACF anticipates this upgrade and the 19 security control findings to be remediated and completed by the end of calendar year (CY) 2024.

Since the end of FY 2022, ACF has made considerable investment in the Next Generation Secure Cloud (NGSC) infrastructure project, which automates code management and includes progressively more intrusive automatic testing and scanning of code beginning in development environments. Applications hosted in NGSC inherit, by default, encryption at rest and in flight, user and application monitoring and logging, network isolation, and active traffic monitoring. ACF's change management process ensures that vulnerability scanning of applications is conducted in non-production environments before that application is promoted to a production environment and made accessible to the general public. Any change to an application's code is tested via vulnerability scanning to determine whether the code change negatively impacts the application's security posture. Another vulnerability scan of the code is conducted immediately after the application code change has been executed in the production environment.

Recommendation 3:
We recommend that ACF update its cloud security procedures to include detailed steps for operational staff to effectively implement cloud security baselines in accordance with HHS requirements.

Response: ACF concurs with this recommendation.

ACF's efforts to update the cloud security procedures to include detailed steps for operational staff to effectively implement cloud security baselines in accordance with HHS requirements remains ongoing. Since May 2022, all of ACF's cloud assets have a baseline of security and performance monitoring capabilities installed when provisioned, with Defense Information Systems Agency Security Technical Implementation Guides and/or Center for Internet Security

benchmarks being the default for servers. Each server instance has security groups configured specifying the traffic to permit (or deny) into and out of the server, complementing the network security provided by network firewalls, web application firewalls, and load balancers. No default administrative accounts are used on these assets. Patching and software upgrades are done routinely and out of cycle if warranted. All application changes that a program requests to be pushed to production must show evidence of a security scan with an acceptable level of risk. As applications move into the NGSC, ACF expects many of these activities, including detailed steps to effectively implement cloud security baselines in accordance with HHS requirements, to be automatically enforced with minimal to no human intervention or error. Further, since October 2022, ACF has acquired and deployed tools that aid in assuring secure components are deployed within the infrastructure. These tools provide endpoint detection and response, application and operating system performance monitoring, and audit log collection capabilities, among other utilities that provide safeguards for the cloud assets, such as file integrity monitoring and facilitating the consistent deployment of secured and compliant assets.

Recommendation 4:
We recommend that ACF leverage cloud security assessment tools to identify misconfigurations and weak cybersecurity controls in its cloud infrastructure.

Response: ACF concurs with this recommendation.

ACF has acquired several products that will aid in identifying misconfigurations of its cloud assets since HHS OIG's audit period of April–May 2022. In October 2022, ACF acquired and deployed security assessment tools that provide endpoint detection and response, file integrity, passive and dynamic code scanning, and capabilities extended across ACF cloud and on-prem environments. As these capabilities continue to be phased in throughout CY 2024, ACF will have more automated means of detecting misconfigurations and weak cybersecurity controls.

Recommendation 5:
We recommend that ACF conduct testing of its cloud information systems that includes the emulation of an adversary's tactics and techniques on a defined reoccurring basis.

Response: ACF concurs with this recommendation.

In July 2021, ACF incorporated testing of its cloud information systems into its continuous monitoring and assessment processes using Synack, a penetration testing service, through HHS. Moreover, since May 2022, ACF OCIO has leveraged HHS services for annual application penetration testing aimed at giving the security team real time visibility into exploitable vulnerabilities across a variety of our assets such as web applications, application programming interfaces, and hosts. In November 2023, ACF expanded its vulnerability monitoring capabilities by deploying an active web application scanning tool, which includes much more extensive configuration testing and more aggressive vulnerability detection of ACF's cloud information systems than the traditional web application scanning that had been in place before.

Again, I appreciate the opportunity to review and comment on this draft report. Please direct any follow-up inquiries 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