Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PENETRATION TEST OF THE ADMINISTRATION FOR CHILDREN AND FAMILIES' COMPUTER NETWORKS AND EXTERNAL WEB APPLICATIONS

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

Thomas M. Salmon
Assistant Inspector General
for Audit Services

September 2015
A-18-14-30330

Office of Inspector General

http://oig.hhs.gov

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

Office of Audit Services

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

Office of Evaluation and Inspections

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

Office of Investigations

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

Office of Counsel to the Inspector General

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

Although our penetration testing did not result in unauthorized access to the Administration for Children and Families' network, we identified three areas of vulnerability that, if addressed, could strengthen the security of its external Web applications and wireless networks.

This summary report provides an overview of the results of our audit of the Administration for Children and Families' (ACF) external Web applications and wireless networks. It does not include specific details of the vulnerabilities that we identified because of the sensitive nature of the information. We have provided more detailed information and recommendations to ACF so that it can address the issues we identified. The findings listed in this summary reflect a point in time regarding system security and may have changed since we reviewed these systems.

WHY WE DID THIS REVIEW

Computer hackers are increasingly compromising Government systems, publishing sensitive data, and using stolen data to commit fraud. Threats to Federal agency computer networks and Web applications are continually changing because of advances made by hackers, the release of new technology, and the deployment of increasingly complex systems. Web sites that are not properly secured are vulnerable to unauthorized users who could compromise the confidentiality of sensitive information or negatively affect the operations of Federal agencies.

ACF's information technology investments include systems that support operations for grants management, child support enforcement, foster care and adoption programs, and Head Start programs. Some of these systems (1) support the collection and processing of personally identifiable information, such as names and Social Security numbers of individuals and families receiving assistance under ACF programs; (2) interface with other Federal and State agency systems; and (3) provide essential data to assist law enforcement and to help reduce costs in Federal and State programs.

Our objective was to determine whether ACF's external Web applications and network were vulnerable to compromise through cyber attacks.

HOW WE CONDUCTED THIS REVIEW

We assessed the ACF network's exposure to cyber attacks by performing penetration testing of its network and Internet-facing systems. Penetration testing is an authorized attempt to locate and exploit vulnerabilities. The purpose of our testing was to determine whether the ACF network could be exploited so that unauthorized users could execute commands on ACF systems.

We conducted penetration testing from July 10 through September 19, 2014, with the knowledge and permission of ACF officials. We requested that ACF's incident response staff not be notified of our testing to assess the effectiveness of ACF's intrusion detection and response controls.

We conducted the performance audit described here 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.

WHAT WE FOUND

Although we did not obtain unauthorized access to the ACF network, we identified issues that could lead to a cyber security incident involving ACF systems and data, given enough time and persistence by malicious computer hackers. We identified vulnerabilities in two primary areas:

- Web applications—We identified Web application vulnerabilities on selected ACF external Web applications. Our testing revealed a total of 240 Web application vulnerabilities on ACF Web applications. We analyzed the results, reviewed the analysis with ACF, and summarized the vulnerabilities into 31 weakness categories.

- Wireless networks—We identified 3 vulnerabilities on ACF's wireless networks.

WHAT WE RECOMMENDED

We made detailed recommendations to ACF that address the Web application and wireless network vulnerabilities we identified. We shared with ACF information about our vulnerability scan findings immediately following the scan and informed ACF about other preliminary findings in advance of issuing our draft report. These recommendations should further strengthen the information security of ACF's external Web applications and wireless networks. Because of the sensitive nature of our findings, we have not listed the detailed recommendations in this summary report.

ACF COMMENTS

In written comments to our draft report, ACF concurred with all of our recommendations and described actions it has taken and plans to take to implement them.