Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

CALIFORNIA IMPLEMENTED SECURITY CONTROLS OVER THE WEB SITE AND DATABASES FOR ITS HEALTH INSURANCE EXCHANGE BUT COULD IMPROVE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

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

April 2015
A-09-14-03005

Office of Inspector General

https://oig.hhs.gov

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

California implemented security controls over the Web site and databases for its health insurance exchange. However, improvements are needed to fully comply with Federal requirements and to increase protection of personally identifiable information.

This summary report provides an overview of the results of our audit of the information security controls at California's health insurance exchange, Covered California. 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 Covered California so that it can address the issues we identified.

WHY WE DID THIS REVIEW

Under provisions of the Patient Protection and Affordable Care Act (ACA),[1] California was the first State to enact legislation creating a health insurance exchange (commonly referred to as a "marketplace"). The Federal Government awarded California $910 million to fund the development of a State-based marketplace, which is known as Covered California. Covered California's Web site offers individuals, families, and small businesses a one-stop shopping portal to find health insurance coverage. Covered California uses databases to store personally identifiable information (PII). As of June 30, 2014, Covered California had processed 882,822 applications for approximately 1.3 million individuals and 1,494 employers.

One of the top challenges in the U.S. Department of Health and Human Services, Office of Inspector General's list of management challenges facing the Department is ensuring security of the marketplaces. Because the marketplaces handle consumers' PII, security of the marketplaces' data and systems is paramount. This review is one of a series of reviews of State-based marketplaces' security controls.

Our objective was to determine whether Covered California had implemented security controls to protect PII on its Web site and databases in accordance with Federal requirements.

HOW WE CONDUCTED THIS REVIEW

We reviewed Covered California's information security controls in place as of June 2014, which included reviewing applicable policies and procedures and interviewing Covered California personnel responsible for the security plan. We also reviewed and analyzed Covered California's risk assessment of the information system and information it processes, stores, or transmits; reviewed its process for identifying vulnerabilities; tested its patch management process for operating systems, Web servers, and software; and performed and reviewed vulnerability scans of certain Web applications and databases.

Our review of applicable Federal requirements included reviewing certain Centers for Medicare & Medicaid Services (CMS) requirements in the *Minimum Acceptable Risk Standards for*

[1] The Patient Protection and Affordable Care Act, P.L. No. 111-148 (Mar. 23, 2010), as amended by the Health Care and Education Reconciliation Act of 2010, P.L. No. 111-152 (Mar. 30, 2010), is known as the Affordable Care Act.

Exchanges (August 1, 2012) Document Suite.[2] These requirements and standards include those related to security plans and risk assessments, vulnerability scanning and penetration testing, patch management and flaw remediation, plan of action and milestones, and incident response.

We limited our review at Covered California to implementation of certain controls over the security of its Web site and three of its databases. We did not review Covered California's overall internal controls. We performed our fieldwork at the Covered California and California Healthcare Eligibility, Enrollment, and Retention System offices in Sacramento, California, from June to September 2014.

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 provided a reasonable basis for our findings and conclusions based on our audit objectives.

WHAT WE FOUND

Covered California had implemented security controls, including policies and procedures, to protect PII on its Web site and databases. However, it did not always comply with Federal requirements. Specifically, Covered California had not performed a vulnerability scan in accordance with Federal requirements, and Covered California's security plan did not meet some of CMS's minimum requirements for protection of marketplace systems. In addition, Covered California did not have secure settings for some user accounts.

Although we did not find evidence that the weaknesses had been exploited, exploitation could result in unauthorized access to and disclosure of PII, as well as disruption of critical marketplace operations. As a result, the weaknesses were collectively and, in some cases, individually significant and could have potentially compromised the integrity of the marketplace.

WHAT WE RECOMMENDED

We recommended that Covered California implement our detailed recommendations to address the findings that we identified related to the vulnerability scan, security plan, and user account settings.

COVERED CALIFORNIA COMMENTS

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

[2] The Document Suite includes *Minimum Acceptable Risk Standards for Exchanges—Exchange Reference Architecture Supplement, Catalog of Minimum Acceptable Risk Controls for Exchanges—Exchange Reference Architecture Supplement*, and *ACA System Security Plan Procedures.*