Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

HEALTH INSURANCE MARKETPLACES GENERALLY PROTECTED PERSONALLY IDENTIFIABLE INFORMATION BUT COULD IMPROVE CERTAIN INFORMATION SECURITY CONTROLS

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

Daniel R. Levinson
Inspector General

September 2014
A-18-14-30011

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.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at https://oig.hhs.gov

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

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.

This summary report provides an overview of the results of three reviews of the security of certain information technology at the Federal, Kentucky, and New Mexico Health Insurance Marketplaces. These reviews generally examined whether information security controls were implemented in accordance with relevant Federal requirements and guidance and whether vulnerabilities identified by prior assessments were remediated in a timely manner.

Although the Centers for Medicare & Medicaid Services (CMS) had implemented controls to secure Healthcare.gov and consumer personally identifiable information (PII) on the Federal Marketplace, we identified areas for improvement in its information security controls. Kentucky had sufficiently protected PII on its Marketplace Web sites and databases in accordance with Federal requirements. However, opportunities to improve the Kentucky Marketplace's database access and information security controls remain. Although New Mexico management had implemented security controls, policies, and procedures to prevent vulnerabilities in its Web site, database, and supporting information systems, its information technology policies and procedures did not always conform to Federal requirements to secure sensitive information stored and processed by the New Mexico Marketplace.

This summary 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 officials of the three Marketplaces so the issues we identified could be appropriately addressed. Part I of this summary provides general background information; Part II summarizes the findings and recommendations of each individual Marketplace review, as well as the responses of the Marketplaces to our findings and recommendations.

On September 4, 2014, CMS issued a statement regarding an intrusion on a server that supports testing of Healthcare.gov but does not contain consumer personal information. The intrusion occurred after the period of our audit and involved technology outside our audit scope.

PART I: BACKGROUND

OIG INFORMATION SYSTEM SECURITY OVERSIGHT

Web sites and database systems that are not secured properly create vulnerabilities that could be exploited by unauthorized persons to compromise the confidentiality of PII or other sensitive data. The integrity of data and systems is a priority for the Office of Inspector General (OIG), and we continually list it as one of the top management challenges facing the U.S. Department of Health and Human Services (Department). In previous work, OIG identified vulnerabilities in a variety of information systems controls, including implementation of requirements and guidance on information security controls, access controls, and configuration management controls, which might have led to unauthorized access to and disclosure of sensitive information or disruption of critical operations. Since the Marketplaces handle consumers' PII, security of the Marketplaces' data and systems is vital.

HEALTH INSURANCE MARKETPLACES

The Marketplaces, also known as the Health Insurance Exchanges, include Federal, State, and Partnership Marketplaces, each of which must implement and successfully operate a complex set of program requirements. Individuals use the Marketplaces to get information about their health insurance options, be assessed for eligibility for enrollment in a health plan and for financial assistance programs, and enroll in the health plan of their choice.

Under the Affordable Care Act (ACA), States have the option of establishing either a State-run Marketplace (State Marketplace), in which the State is responsible for core Marketplace functions, or a State-partnership marketplace (Partnership Marketplace), in which the Department and the State share responsibilities for core functions.[1] ACA requires the Federal Government to operate a Federally Facilitated Marketplace (FFM) in States that elect not to operate a State or Partnership Marketplace. CMS operates the FFM, known as Healthcare.gov, and works with States on the operation of State and Partnership Marketplaces. In addition to providing for Marketplaces for individual insurance, ACA provides for the establishment of Small Business Health Options Program (SHOP) Marketplaces to help businesses provide health insurance for their employees.[2]

Effective operation of the Marketplaces requires rapid, accurate, and secure integration of data from numerous Federal and State sources and from individuals who use the Marketplaces. It also requires an established, large-scale means of communication among many Federal and State systems.

DATA AND SYSTEMS SECURITY

Federal Regulations To Protect Personally Identifiable Information

On March 27, 2012, CMS issued a final rule,[3] codified at 45 CFR parts 155, 156, and 157, providing that a Marketplace may not create, collect, use, or disclose any PII needed to perform minimum functions unless it does so in a manner consistent with Federal privacy and security standards. The final rule established additional requirements, including standards related to (1) monitoring, periodically assessing, and updating security controls and (2) developing and using secure electronic interfaces. On August 30, 2013, CMS issued a final rule,[4] codified at 45 CFR parts 147, 153, 155, and 156, that established standards for health insurance issuers participating on the Marketplaces. The final rule established standards to protect and secure the individuals' PII.

Privacy and Security Requirements

Federal regulations require that the Department oversee the Marketplaces and non-Exchange (non-Marketplace) entities that are required to comply with the privacy and security standards

[1] P.L. 111-148, section 1321 (42 USC 18041).
[2] ACA §1311(b)(1)(B).
[3] 77 Fed. Reg. 18310 (March 27, 2012).
[4] 78 Fed. Reg. 54070 (August 30, 2013).

established and implemented by each Marketplace. These privacy and security standards, found at 45 CFR §§ 155.260 and 155.280, are based on the following principles:

- *Individual access.* Individuals should be able to access and obtain their PII easily and in a readable format.

- *Correction.* Individuals should be able to dispute the accuracy or integrity of their PII in a timely manner and to have erroneous information corrected or to have a dispute documented if their requests for correction are denied.

- *Openness and transparency.* There should be openness and transparency about policies, procedures, and technologies that directly affect individuals or their PII.

- *Individual choice.* Individuals should be able to make informed decisions about the collection, use, and disclosure of their PII.

- *Collection, use, and disclosure limitations.* PII should be created, collected, used, and disclosed only to the extent necessary to accomplish specified purposes and never to discriminate.

- *Data quality and integrity.* Persons and entities should take reasonable steps to ensure that PII is complete, accurate, and up to date to the extent necessary for the person's or entity's intended purpose and that it has not been altered or destroyed in an unauthorized manner.

- *Safeguards.* PII should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

- *Accountability.* These principles should be implemented, and adherence assured, through appropriate monitoring and other means, and there should be methods to report and mitigate nonadherence and breaches.

Protecting and ensuring the confidentiality, integrity, and availability of Marketplace enrollment information and information systems is the responsibility of the Marketplaces. To facilitate compliance with the security requirements for the Marketplaces (Federal, State, and Partnership), CMS developed the *Minimum Acceptable Risk Standards for Exchanges—Exchange Reference Architecture Supplement (*MARS-E),[5] which defines minimum standards for acceptable security risk. MARS-E outlines specific security controls, policies, and procedures that protect the confidentiality, integrity, and availability of a system and its information.

The National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems. CMS incorporated NIST guidelines into MARS-E.

[5] Version 1, August 1, 2012.

Security controls are the safeguards and countermeasures that are designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by information systems. Security controls describe the specific capability or function a system needs to protect a particular aspect of the system from unauthorized use. Controls often safeguard the system from potential future vulnerabilities or remediate current vulnerabilities. Vulnerabilities can range from a flaw or weakness in a system's security procedures (e.g., outdated system security plans), design (e.g., erroneous computer code), implementation (e.g., missing critical patches[6]), or internal controls (e.g., failing to perform routine virus scans) that could result, accidentally or intentionally, in a security breach or the violation of an organization's security policy.

All information systems face vulnerabilities, and complex systems operate at a certain level of risk. Not all vulnerabilities lead to security breaches or high threat risks. An organization's information systems security staff should employ risk management processes to identify vulnerabilities, assess the level of risk a particular vulnerability presents to the overall security of the system, and devise and implement an action plan to correct the vulnerability on the basis of the determined level of risk. Vulnerabilities identified as high risk should be corrected as soon as possible because of their potentially severe or catastrophic impact on the system in case of a breach. Even if a high level of risk has been identified, the system may continue to operate while immediate action is taken. The detection of system vulnerabilities does not necessarily mean a system is not safe. A soundly engineered and secure system, coupled with a rigorous risk management and mitigation process, is the best way to operate a safe system.

Methodology

Various methods exist to determine whether a system is operating securely. Our reviews included determining the adequacy of the information security general controls and performing or reviewing results of vulnerability scans of Web applications and databases.

Review of Information Security General Controls. The primary objectives of general controls are to safeguard data, protect computer application programs, prevent unauthorized access to system software, and ensure continued operations in case of unexpected interruptions. Reviewing an organization's written policies and procedures, including its systems security plan, can help to identify ineffective policies and procedures to reduce risk that could jeopardize an organization's mission, information, and information technology assets. System security plans should include updated policies and procedures related to regular security testing to measure compliance in areas such as patch management, password policy, and configuration management; incident detection, reporting, and response processes, including conducting regular risk assessments; and maintaining proper documentation.

Web Application Vulnerability Scan. Web application vulnerability scans identify potential security vulnerabilities in the Web application and architectural design. Scanners simulate an outside malicious attack on the system and may identify system vulnerabilities that could put a

[6] Patches are additional pieces of computer code developed by software vendors to address problems (commonly called bugs) found in software.

system's security at risk. Scanners use the same techniques as hackers, so the scanners test the security from an outside perspective.

Database Vulnerability Scan. Database vulnerability scans identify potential security vulnerabilities in a system's databases that store sensitive information, including PII. Scanners simulate an outside malicious attack on the system and may identify system vulnerabilities that could put a system's security at risk. Scans allow security assessors to determine how effectively the data are being protected.

OBJECTIVE AND LIMITATIONS

The objective of our reviews was to determine whether the selected Marketplaces had protected the sensitive information processed and stored by the Web sites, databases, and supporting information systems. We reviewed the implementation of certain controls supporting the security of the Marketplaces' Web sites and supporting databases. We did not review the systems' overall internal controls and did not determine whether the overall systems were secure.

The findings listed in this summary document reflect a point in time regarding system security and may have changed since we reviewed these systems. Our State reviews are not projectable to other States.

We conducted these performance audits in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audits 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.

FUTURE OIG WORK

We will issue a series of reports on the Marketplaces' data and system security for the current and future Marketplace stages. Reports on the FFM and the State Marketplaces of New Mexico and Kentucky are the first three in this series. We are also following up on the implementation of recommendations made in these reports by CMS and the State Marketplaces.

PART II: SUMMARIES OF REPORTS

CMS'S HEALTHCARE.GOV WEB SITE

BACKGROUND

The FFM operates through CMS's Healthcare.gov Web site. Healthcare.gov also serves as a gateway for consumers to reach State Marketplaces.

HOW WE CONDUCTED THIS REVIEW

We reviewed information security controls and completed a Web application vulnerability scan of Healthcare.gov. We conducted our overall audit work from February to June 2014, including vulnerability scans and simulated attacks in April and May.

Scope

We focused our audit on information security controls over certain operations and systems that support the FFM's Web site and the FFM database servers containing PII.[7] We also reviewed CMS's information security policies and procedures. We reviewed contractor reports related to prior vulnerability scans of the FFM and its supporting databases, assessed whether CMS has fully addressed and remediated the vulnerabilities found, and conducted a Web site vulnerability scan[8] using a commercial automated Web site vulnerability scanner and other open source tools. We limited our review of controls to those that were in effect at the time of our audit.

Methodology

To accomplish our objective, we:

- reviewed applicable Federal requirements,
- interviewed CMS officials responsible for monitoring the FFM to help determine whether CMS complied with Federal requirements,
- reviewed CMS staff and contractor documentation to determine whether it complied with Federal requirements,
- conducted Web site vulnerability scanning and simulated attacks against Healthcare.gov during April and May 2014,

[7] We did not review any systems outside the FFM that contain consumer information. The Department also stores some consumer information in a system (Multidimensional Insurance Data Analytics System (MIDAS)) that resides outside Healthcare.gov. We will be conducting an information technology security review of this system.
[8] Our Web site scan covered only Healthcare.gov, the public interface for consumer enrollment and eligibility.

- reviewed CMS security control assessment reports and vulnerability scan reports related to the FFM and supporting databases to determine whether findings had been tracked and vulnerabilities remediated,

- interviewed CMS staff and contractors about their procedures for securing the FFM, and

- discussed our testing procedures and findings with CMS.

WHAT WE FOUND

Since the launch of Healthcare.gov on October 1, 2013, CMS has taken actions to lower the security risks associated with Healthcare.gov systems and consumer PII, including, but not limited to:

- establishing a dedicated security team under the Chief Information Officer to monitor and track corrective action plans for vulnerabilities and ensure they are completed,

- performing weekly vulnerability scans of FFM-related systems, and

- completing two security control assessments of the FFM.

Although CMS had implemented controls to secure Healthcare.gov and consumer PII data, we identified areas for improvement. At the time of our review, CMS had not:

- implemented a process to use automated tools to test database security configuration settings on all of its supporting databases,

- implemented an effective enterprise scanning tool to test for Web site vulnerabilities,

- maintained adequate documentation to verify that a finding from one of its FFM security control assessment reports related to a database property file containing user credentials had been sufficiently closed by encrypting the file with a Federal Information Processing Standard (FIPS) 140-2-approved cryptographic module, and

- detected and defended against our Web site vulnerability scanning and simulated cyber attacks directed at the Healthcare.gov Web site.

The Web application vulnerability scanning that we conducted revealed one critical vulnerability in Healthcare.gov, which we confirmed with CMS.[9] CMS stated that it was aware of the vulnerability and had developed a corrective action plan with a scheduled completion date of June 30, 2014. Therefore, the vulnerability had not been fully remediated at the time we

[9] The Web scanning tool describes the relative severity of a vulnerability as follows: critical—an attacker's ability to execute commands on the server or retrieve and modify information; high—a hacker's ability to view source code, files, and messages; medium—issues that could be sensitive; and low—interesting issues or issues that could potentially become more severe.

performed our vulnerability scan. Subsequently, CMS informed us that the recommended remediation was implemented to resolve the vulnerability. We provided the results from the Web site vulnerability scans to CMS so it could analyze the results and start any necessary remediation actions. After our audit, CMS provided written information explaining the steps it took to remediate the vulnerability.

With respect to our review of CMS' server vulnerability scan reports related to the FFM databases, we determined that although CMS was taking action to remediate the vulnerabilities identified in those reports, it had not fully remediated two critical vulnerabilities. CMS explained that it had developed a corrective action plan to resolve the two critical vulnerabilities; however, the vulnerabilities had not yet been fully remediated during our audit. CMS was working with its contractor to schedule a date to remediate one of the two vulnerabilities, and after our audit, CMS stated it had fully remediated the second critical vulnerability. These critical vulnerabilities placed the confidentiality, integrity, and availability of PII at risk and could have allowed unauthorized access to consumer PII.

WHAT WE RECOMMENDED

To ensure that consumer PII data entered on Healthcare.gov is secure and protected, we recommended that CMS management address the findings we identified.

CMS COMMENTS AND OIG RESPONSE

In written comments, CMS concurred with all of our recommendations and described the actions it has taken and plans to take to implement them. However, CMS stated that it did not believe that the finding and recommendation related to encrypting files using an encryption module that has been FIPS 140-2 validated should be included because the actions it has taken to resolve the issue were sufficient. Although CMS had implemented controls to mitigate risks related to the finding, we did not receive supporting documentation to verify FIPS 140-2 compliance during our audit and remain concerned about CMS's use of encryption modules that are not FIPS 140-2 validated. Therefore, we did not change our recommendation.

KENTUCKY HEALTH BENEFIT EXCHANGE

BACKGROUND

The Commonwealth of Kentucky operates a State Marketplace for individuals and small businesses. As of April 21, 2014, the Kentucky Health Benefit Exchange (KHBE) had processed 478,718 applications for approximately 610,891 individuals[10] and 628 employers to enroll 413,410 Kentucky residents in new health coverage, including 330,615 who qualified for Medicaid coverage and 82,795 who purchased private insurance under the ACA.[11]

HOW WE CONDUCTED THIS REVIEW

We reviewed information security controls, completed a Web application vulnerability scan, and completed a database vulnerability scan of KHBE. We performed our fieldwork at the Commonwealth's offices in Frankfort, Kentucky, from April to May 2014.

Scope

We reviewed the Commonwealth policies, procedures, and controls in place as of April 2014. We limited our review to certain CMS MARS-E requirements and NIST guidelines. These requirements, safeguards, and standards included these topics:

- security plan,
- risk assessment,
- vulnerability scanning,
- penetration testing,
- patch management and flaw remediation,
- plan of action and milestones (POA&M), and
- incident response.

We focused our review on the Commonwealth's KHBE Web sites, databases, and supporting systems. We did not review the Commonwealth's internal controls as a whole.

[10] An application may contain one or more individuals.
[11] http://governor.ky.gov/healthierky/Pages/default.aspx. Accessed on April 30, 2014.

Methodology

To accomplish our objectives, we assessed the KHBE:

- policies and procedures;
- system security plan;
- risk assessment;
- network boundaries and connections with other agencies;
- encryption methods used to protect data on and between Web sites and databases;
- capabilities for identifying vulnerabilities;
- patch management process for operating systems, Web servers, and software;
- Web sites and databases using automated audit tools; and
- vulnerability scans between August 2013 and March 2014.

We judgmentally selected for review:

- KHBE's security incident related to PII that was reported to the Commonwealth's Office of Technology,
- the 6 databases that contained KHBE data,
- KHBE's 2 Web sites for vulnerabilities assessment, and
- all 95 servers used for KHBE that contained Marketplace data.

WHAT WE FOUND

The Commonwealth had sufficiently protected PII on its KHBE Web sites and databases in accordance with Federal requirements. In general, the Commonwealth, using encryption, secured individuals' PII as it was entered into the Commonwealth's KHBE Web sites and while it was stored within the Commonwealth's database or during transmission. However, opportunities to improve KHBE database access and information security controls remain. Specifically, the Commonwealth had not sufficiently restricted user and group access to authorized roles and functions and had not sufficiently addressed Federal requirements for its system security planning, risk assessment, penetration testing and flaw remediation, POA&M, and incident response capability.

These conditions existed because the Commonwealth was transitioning its information technology responsibilities among agencies and had not sufficiently established coordination between them. In addition, at the time of our review, the Commonwealth agencies supporting the KHBE had not sufficiently implemented certain policies and procedures to meet Federal requirements. As a result, the PII on 478,718 applications for approximately 610,891 individuals and 628 employers was at a greater risk of being exploited.

WHAT WE RECOMMENDED

We recommended that Commonwealth management address the findings we identified.

COMMONWEALTH COMMENTS AND OIG RESPONSE

In its comments, the Commonwealth concurred with most of our recommendations and partially concurred with one recommendation. Although the Commonwealth partially concurred with our recommendation to limit access to its databases by restricting access to certain roles and functions, it stated that it would further explore the risks and determine whether it needed to restrict that access further. In a separate comment, the Commonwealth said that it concurred with our recommendation to perform penetration testing and asserted that it had "performed regular vulnerability and penetration [testing] for every major release."

Restricting database access to those with certain roles and functions increases the level of overall security for PII. Regarding the Commonwealth comment on penetration testing, although the Commonwealth had performed vulnerability assessments on KHBE-related applications, it had not performed external network penetration testing per Federal requirements. To clarify, vulnerability assessments are used to search for weaknesses or exposures, and penetration testing is used to attempt to gain access to resources without knowledge of usernames, passwords, or other normal means of controlling access.

NEW MEXICO HEALTH INSURANCE EXCHANGE

BACKGROUND

The New Mexico Health Insurance Exchange (NMHIX) is a partnership exchange and operates its own Marketplace Web site, nmhix.com. NMHIX operates a SHOP, which enrolls small businesses, but directs individuals to enroll through the FFM for health insurance.

HOW WE CONDUCTED THIS REVIEW

We reviewed information security controls, completed a Web application vulnerability scan, and completed a database vulnerability scan of NMHIX. We conducted our audit work during March 2014.

Scope

We focused our audit on NMHIX's Web site, database, and other supporting information systems. We reviewed NMHIX's implementation of CMS minimum information security requirements for State health insurance exchanges and NIST guidelines within the following information technology operational areas: wireless network administration, Universal Serial Bus port and device management, mobile device management, data encryption, remote access, patch management, Web applications, and database applications. We limited our review to these security control areas and to controls that were in place at the time of our site visit. We did not review NMHIX's internal controls as a whole.

Methodology

To accomplish our objective, we:

- reviewed applicable Federal and State requirements, NIST recommendations, and industry best practices;
- interviewed appropriate computer operations personnel responsible for information security;
- judgmentally selected systems and tested their hardware and software configurations;
- analyzed system configuration reports for potential network vulnerabilities, such as incomplete patching;
- performed wireless scans (without capturing or reading data);
- performed a Web application vulnerability scan on the NMHIX Web site;
- performed a database vulnerability scan on the NMHIX database; and

- discussed our findings with NMHIX management.

WHAT WE FOUND

Although NMHIX had implemented security controls, policies, and procedures to prevent vulnerabilities in its Web site, database, and supporting information systems, NMHIX's information technology policies and procedures did not always conform to Federal information technology requirements and NIST recommendations to secure sensitive information stored and processed by NMHIX. These vulnerabilities placed consumer data collected on the NMHIX Web site at risk.

Specifically, our audit identified the following vulnerabilities:

- one data encryption vulnerability,
- two remote access vulnerabilities,
- one patch management vulnerability, and
- one Universal Serial Bus port and device vulnerability.

In addition, our Web application vulnerability scan of the NMHIX Web site revealed 64 vulnerabilities. The tool we used for the scan classified the vulnerabilities as critical (2), high (2), medium (4), and low (56). We described the definitions for the severity of the vulnerabilities in footnote 9.

Our database vulnerability scan of the NMHIX database, which stores all sensitive user data, revealed 74 vulnerabilities. The tool we used for the scan classified the vulnerabilities as high (1), medium (44), and low (29).[12]

The vulnerabilities we identified placed the confidentiality, integrity, and availability of NMHIX information at risk and could have allowed unauthorized access to sensitive consumer data.

WHAT WE RECOMMENDED

We recommended that NMHIX management address the vulnerabilities we identified.

[12] The database scanning tool describes the relative severity of a vulnerability as follows: high—typically allows a nonprivileged user or nonuser to potentially gain full, unauthorized access to or crash the application, database, or system; medium—typically allows a limited-privileged user to potentially gain unauthorized access to or crash the application, database, or system; and low—typically allows a privileged user to potentially gain unauthorized access to or crash the application, database, or system.

NEW MEXICO HEALTH INSURANCE EXCHANGE COMMENTS AND OIG RESPONSE

In written comments, NMHIX concurred with all of our recommendations and described the actions it had taken and plans to take to implement them.