Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

OBSERVATIONS NOTED DURING THE OIG REVIEW OF CMS'S IMPLEMENTATION OF THE HEALTH INSURANCE EXCHANGE—DATA SERVICES HUB

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

Gloria L. Jarmon
Deputy Inspector General

August 2013
A-18-13-30070

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.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20201

August 2, 2013

TO: Marilyn Tavenner
Administrator
Centers for Medicare & Medicaid Services

Tony Trenkle
Chief Information Officer
Centers for Medicare & Medicaid Services

FROM: /Gloria L. Jarmon/
Deputy Inspector General for Audit Services

SUBJECT: Memorandum Report: Observations Noted During the OIG Review of CMS's Implementation of the Health Insurance Exchange—Data Services Hub (A-18-13-30070)

This memorandum report provides the results of our review of the Centers for Medicare & Medicaid Services' (CMS) implementation of the Data Services Hub (Hub) from a security perspective. To determine the status of the implementation of the Hub, we assessed the information technology (IT) security controls that CMS is implementing for the Hub, adequacy of the testing activities being performed during its development, and the coordination between CMS and Federal and State agencies during the development of the Hub. A memorandum report is the best vehicle to communicate the results of our performance audit work when observations, not recommendations, are the key elements of our results.

SUMMARY

CMS is addressing and testing security controls of the Hub during the development process. However, several critical tasks remain to be completed in a short period of time, such as the final independent testing of the Hub's security controls, remediating security vulnerabilities identified during testing, and obtaining the security authorization decision for the Hub before opening the exchanges. CMS's current schedule is to complete all of its tasks by October 1, 2013, in time for the expected initial open enrollment period.

BACKGROUND

States must establish health insurance exchanges by January 1, 2014,[1] and all health insurance exchanges must provide an initial open enrollment period beginning October 1, 2013 (45 CFR § 155.410). Health insurance exchanges are State-based competitive marketplaces where individuals and small businesses will be able to purchase private health insurance. Exchanges will serve as a one-stop shop where individuals will get information about their health insurance options, be assessed for eligibility (for, among other things, qualified health plans, premium tax credits, and cost sharing reductions), and enroll in the health plan of their choice. A State may elect to operate its own State-based exchange or partner with the Federal Government to operate a State partnership exchange. If a State elects not to operate an exchange, the Department of Health and Human Services will operate a Federally Facilitated Exchange.[2] For the purposes of this report, "exchanges" refers to all three types of health insurance exchanges.

The Hub is intended to support the exchanges by providing a single point where exchanges may access data from different sources, primarily Federal agencies. It is important to note that the Hub does not store data. Rather it acts as a conduit for exchanges to access the data from where they are originally stored. The functions of the Hub will include facilitating the access of data by exchanges; enabling verification of coverage eligibility; providing a central point for the Internal Revenue Service (IRS) when it asks for coverage information; providing data for oversight of the exchanges; providing data for paying insurers; and providing data for use in Web portals for consumers.

Effective security controls are necessary to protect the confidentiality, integrity, and availability of a system and its information. The National Institute of Standards and Technology (NIST) developed information security standards and guidelines, including minimum requirements for Federal information systems. CMS is required to follow the NIST security standards and guidelines in securing the Hub.[3]

OBJECTIVE, SCOPE, AND METHODOLOGY

Our primary audit objective was to determine CMS's current progress in implementing security requirements for the Hub. We evaluated the adequacy of the development and testing of the Hub from a security perspective. We did not review the functionality of the Hub.

[1] The Patient Protection and Affordable Care Act § 1311(b) (P.L. No. 111-148) and the Health Care Reconciliation Act of 2010 (P.L. No. 111-152), collectively known as the Affordable Care Act (ACA).

[2] The Center for Consumer Information and Insurance Oversight Web site has further information on the health insurance exchanges: http://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces. Accessed on July 9, 2013.

[3] NIST's security standards assist Federal agencies in implementing the requirements under the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541, *et seq*.

To accomplish our objectives, we:

- reviewed documentation, System Development Life Cycle artifacts, and CMS project schedules and timelines (including milestones established by CMS) as of March and May 2013 (the dates of CMS's two project schedules) to track the activities that need to be completed before the implementation of the Hub;
- interviewed CMS employees and contractors;
- interviewed personnel from key Federal agencies working with CMS during the development of the Hub; and
- reviewed CMS's security testing results.

We performed our fieldwork substantially from March through May 2013.

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.

RESULTS

At the time of our review, CMS and its contractors were continuing to develop the Hub and work with its Federal and State partners in testing the Hub to ensure its readiness in time for the initial open enrollment to begin on October 1, 2013. We made the following observations on security controls, security testing, and coordination at the time of our fieldwork.

Assessment of Security Controls

According to NIST security standards, every Federal information system must obtain a security authorization before the system goes into production. The security authorization is obtained from a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations.

The security authorization package must include a system security plan (SSP), information security risk assessment (RA), and security control assessment (SCA) report. The security authorization package provides important information about risks of the information system, security controls necessary to mitigate those risks, and results of security control testing to ensure that the risks have been properly mitigated. Therefore, these documents must be completed before the security authorization decision can be made by the authorizing official. The authorizing official may grant the security authorization with the knowledge that there are still risks that have not been fully addressed at the time of the authorization.

CMS incorporated the elements required for adequate security into the draft Hub SSP. The SSP provides an overview of the security requirements of the system and describes the controls in place or planned (e.g., access controls, identification and authentication) for meeting those requirements and delineates the responsibilities and behavior expected of all individuals who access the system. The information security Hub RA was being drafted during our fieldwork. The RA should identify risks to the operations (including mission, functions, image, or reputation), agency assets, and individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. However, the CMS contractor did not expect to provide finalized security documents, including the SSP and RA, to CMS for its review until July 15, 2013. The original dates listed in CMS's March and May 2013 schedules for the contractor to submit the final security documents were May 6, 2013, and July 1, 2013, respectively. Because the documents were still drafts, we could not assess CMS's efforts to identify security controls and system risks for the Hub and implement safeguards and controls to mitigate identified risks.

According to CMS's current timeline, the security authorization decision by the authorizing official, the CMS Chief Information Officer (CIO), is expected on September 30, 2013; the March 2013 schedule reported the date as September 4, 2013. If there are additional delays in completing the security authorization package, the CMS CIO may not have a full assessment of system risks and security controls needed for the security authorization decision by the initial opening enrollment period expected to begin on October 1, 2013.

Adequacy of Security Testing

CMS and its contractors are performing security testing throughout the Hub's development, including vulnerability assessments of Hub services. CMS is logging and tracking defects and vulnerabilities throughout the development process and correcting and retesting Hub services to ensure that vulnerabilities are remediated.

An SCA of the Hub must be performed by an independent testing organization before the security authorization is granted.[4] The SCA determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome of meeting the security requirements for the information system. The goal of the SCA test plan is to explain clearly the information the testing organization expects to obtain prior to the SCA, the areas that will be examined, and the proposed scheduled activities expected to be performed during the SCA. According to CMS's March 2013 schedule, the SCA test plan was scheduled to be provided to CMS for its review on May 13, 2013, and the SCA was scheduled to be performed between June 3 and 7, 2013. However, in the May 2013 schedule, the SCA test plan due date was moved to July 15, 2013, and the SCA is now scheduled to be performed between August 5 and 16, 2013. CMS stated that the SCA was moved so that performance stress testing of the Hub could be finished before the SCA and any vulnerabilities identified during the stress

[4] NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* Revision 1.

testing could be remediated. Otherwise, CMS might need to perform an additional SCA after the remediation was complete.

CMS has 3 weeks between the receipt of the SCA test plan and the start of the SCA for CMS to make changes to the plan and for the independent testing organization to adjust the plan. CMS must ensure that all devices in the Hub environment, including all firewalls and servers, are analyzed during the SCA. In addition, the draft report with the results of the SCA is not due from the contractor performing the SCA until September 9, 2013, and the final report is not due until September 20, 2013. We could not assess planned testing or whether vulnerabilities identified by the testing would be mitigated because the SCA test plan had not been provided and the SCA had not been completed at the time of our review. If there are additional delays in completing the SCA test plan and performing the SCA, the authorizing official may not have the full assessment of implemented security controls needed for the security authorization decision by the initial opening enrollment period expected to begin on October 1, 2013.

See the table for a summary of the key security dates.

Table: Key Hub Security Due Dates

Security Document	Date Due (per March 2013 schedule)	Date Due (per May 2013 schedule)
Final SSP and RA	May 6, 2013	July 1, 2013*
SCA Test Plan	May 13, 2013	July 15, 2013
SCA	June 3-7, 2013	August 5-16, 2013
Draft SCA Report	June 28, 2013	September 9, 2013
Final SCA Report	July 15, 2013	September 20, 2013
Security Authorization Decision	September 4, 2013	September 30, 2013

* On July 1, 2013, CMS stated that the new date for the SSP and RA is July 15, 2013.

Coordination Among CMS and Its Federal and State Partners

CMS is coordinating with its Federal and State partners during the development and testing of the Hub, in part to ensure that security measures are implemented by all stakeholders. The Federal partners are the IRS, Social Security Administration (SSA), Department of Homeland Security (DHS), Veterans Health Administration (VHA), Department of Defense (DOD), Office of Personnel Management (OPM), and Peace Corps.

CMS developed a testing approach for interagency testing and has developed test plans. CMS is in the process of executing its test plans, which include testing for secure communications between CMS and its Federal and State partners and performance stress testing of the Hub.

CMS also developed security-related documents related to the Hub and the exchanges. CMS developed Interface Control Documents (ICD) with all of its Federal partners. The ICDs should be established during the development of new systems. The ICDs provide a common, standard technical specification for transferring ACA-related information between CMS (the Hub) and its Federal partners. The ICDs establish standard rules, requirements, and policies (including security-related policies) with which the development and implementation of the interfaces between CMS and its Federal partner must comply. CMS and its Federal partners collaborated in the development of the ICDs and signed the ICDs in May 2013.

Federal policy requires agencies to develop Interconnection Security Agreements (ISA) for Federal information systems and networks that share or exchange information with external information systems and networks. Specifically, Office of Management and Budget Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their IT systems to other systems. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection. The Master ISA describes the systems' environment, network architecture, and the overall approach for safeguarding the confidentiality, integrity, and availability of shared data and system interfaces. In addition, the Master ISA contains information on CMS information security policy and the roles and responsibilities pertaining to the maintenance of the security of ACA systems.

CMS completed a preliminary review of the Master ISA between CMS and the developer of the Hub on April 2, 2013, and the Associate ISAs on May 15, 2013. Each of the Federal partners will provide similar information pertaining to the partner agency in the Associate ISAs and signed by the Federal partner authorized official. The final review of the ISAs for all Federal partners is scheduled to be completed by September 3, 2013 and the CMS CIO is scheduled to grant the authority to connect to the Hub by September 30, 2013. In addition, CMS has developed a non-Federal ISA for third parties and the States.

A service level agreement (SLA) is a negotiated agreement between a service provider and the customer that defines services, priorities, responsibilities, guarantees, and warranties by specifying levels of availability, serviceability, performance, operation, or other service attributes. A SLA is needed between CMS and each of its Federal partners to establish agreed-upon services and availability, including response time and days and hours of availability of the Hub and the Federal partner's ACA systems. According to CMS's project schedule, the SLA with IRS was completed on March 15, 2013; the SLA with DHS is expected to be signed by July 26, 2013; and the SLA with SSA is expected to be signed by September 27, 2013. The SLAs with the remaining Federal partners (VHA, DOD, OPM, Peace Corps) are expected to be signed by September 20, 2013. The SLAs should be approved by all parties before October 1, 2013.

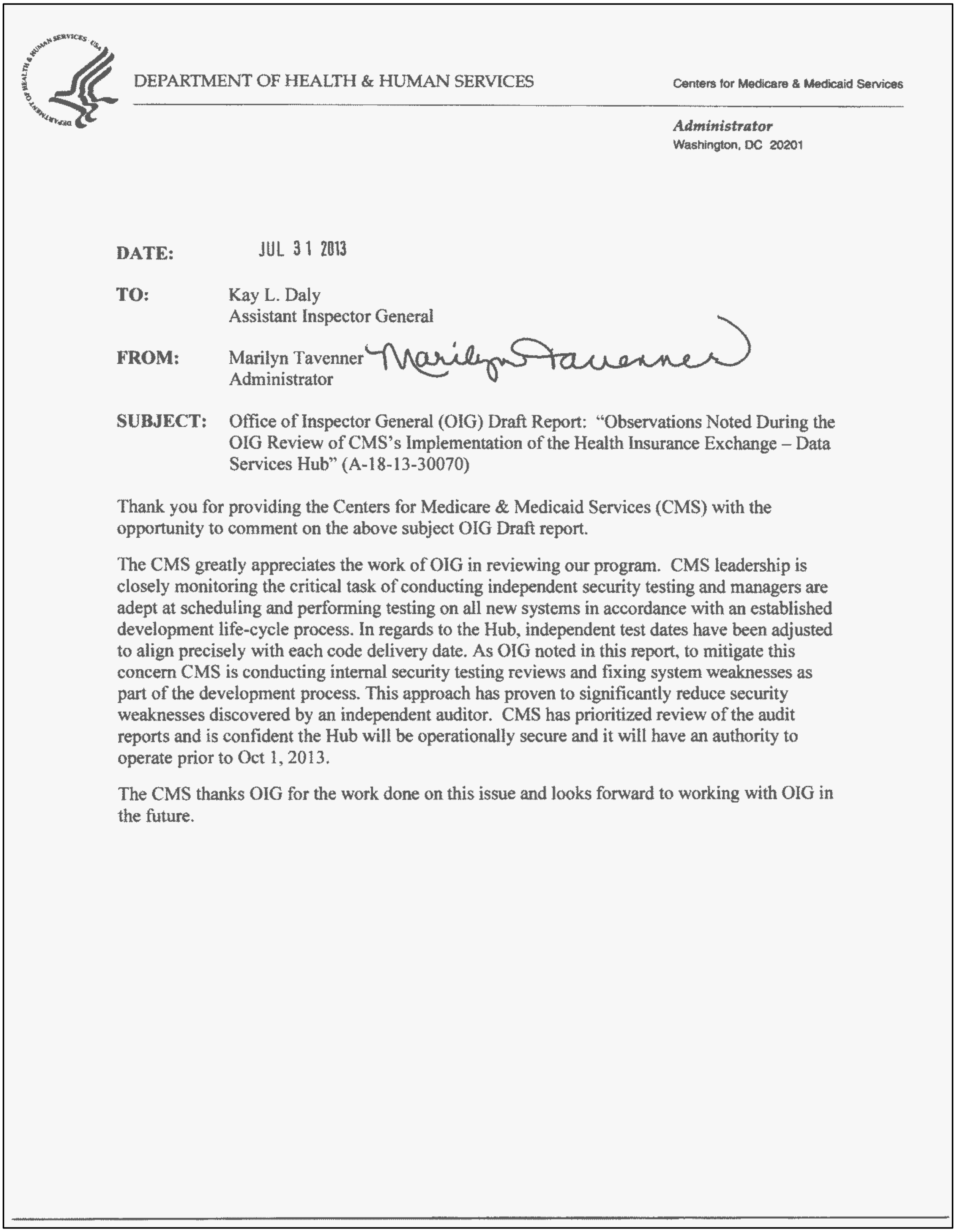
SUMMARY OF OBSERVATIONS

This memorandum report informs stakeholders of the status of steps CMS is taking to ensure that there are adequate security measures for the Hub. CMS is working with very tight deadlines to ensure that security measures for the Hub are assessed, tested, and implemented by the expected initial open enrollment date of October 1, 2013. If there are additional delays in completing the security assessment and testing, the CMS CIO may have limited information on the security risks and controls when granting the security authorization of the Hub.

CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS

In its comments on our draft report, CMS stated that it is confident that the Hub will be operationally secure and it will have a security authorization before October 1, 2013. CMS also provided technical comments, which we addressed as appropriate. We have included CMS's comments in the Appendix.

APPENDIX: CENTERS FOR MEDICARE & MEDICAID SERVICES COMMENTS



DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: JUL 31 2013

TO: Kay L. Daly
Assistant Inspector General

FROM: Marilyn Tavenner Marilyn Tavenner
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: "Observations Noted During the OIG Review of CMS's Implementation of the Health Insurance Exchange – Data Services Hub" (A-18-13-30070)

Thank you for providing the Centers for Medicare & Medicaid Services (CMS) with the opportunity to comment on the above subject OIG Draft report.

The CMS greatly appreciates the work of OIG in reviewing our program. CMS leadership is closely monitoring the critical task of conducting independent security testing and managers are adept at scheduling and performing testing on all new systems in accordance with an established development life-cycle process. In regards to the Hub, independent test dates have been adjusted to align precisely with each code delivery date. As OIG noted in this report, to mitigate this concern CMS is conducting internal security testing reviews and fixing system weaknesses as part of the development process. This approach has proven to significantly reduce security weaknesses discovered by an independent auditor. CMS has prioritized review of the audit reports and is confident the Hub will be operationally secure and it will have an authority to operate prior to Oct 1, 2013.

The CMS thanks OIG for the work done on this issue and looks forward to working with OIG in the future.

Office of Inspector General Note—Technical comments in the auditee's response to the draft have been omitted from the final report and all appropriate changes have been made.