Testimony of:
Kay Daly
Assistant Inspector General for Audit Services
Office of Inspector General, U.S. Department of Health and Human Services
Hearing Title: "The Threat to Americans' Personal Information: A Look Into the Security and Reliability of the Health Exchange Data Hub"
House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
September 11, 2013

Introduction

Good afternoon, Chairman Meehan, Ranking Member Clarke, and other distinguished Members of the Subcommittee. Thank you for the opportunity to testify about the Office of Inspector General's (OIG) review of the Centers for Medicare & Medicaid Services' (CMS) implementation of the Data Services Hub (Hub) from a security perspective, which we issued on August 2, 2013.[1] My testimony today summarizes OIG's observations about CMS's progress in implementing security requirements of the Hub during the period of our review.[2] We assessed the information technology (IT) security controls that CMS was implementing for the Hub, adequacy of the testing being performed during its development, and the coordination between CMS and Federal and State agencies during the development of the Hub. We did not review the functionality of the Hub or issues specific to the Privacy Act.

At the time of our review, CMS was addressing and testing security controls for the Hub during the development process. Several critical tasks remained to be completed, such as the final independent testing of the security controls, remediating security vulnerabilities identified during testing, and obtaining the security authorization decision for the Hub before opening the exchanges. CMS's schedule at that time was to complete all of these tasks by October 1, 2013, in time for the expected initial open enrollment date for health insurance exchanges.

Our report described the timelines that CMS provided us for its system security plan, risk assessment, security control assessment, and security authorization decisions. In our report, we noted that between March and July, some key targets had been shifted to later dates. These were internal target dates set by CMS for these milestones and not mandated deadlines. Since issuing our report, CMS has reported to us that it has made additional progress on these key milestones, including obtaining its security authorization for the Hub on September 6, 2013. We have not independently verified CMS's progress since completing our audit.

Following is a discussion of the Hub's role within the health insurance exchanges, the results of our review, and concluding observations.

---

[1] *Observations Noted During the OIG Review of CMS's Implementation of the Health Insurance Exchange—Data Services Hub*, A-18-13-30070, August 2013, available online at https://oig.hhs.gov/oas/reports/region1/181330070.asp.

[2] We performed our fieldwork substantially from March through May 2013. We continued to receive updates from CMS through July 1, 2013, and its comments on our draft report are included in the final report.

Background

States must establish health insurance exchanges by January 1, 2014,[3] and all health insurance exchanges must provide an initial open enrollment period beginning October 1, 2013 (45 CFR § 155.410). Health insurance exchanges, also known as Marketplaces, are State-based competitive marketplaces where individuals and small businesses will be able to purchase private health insurance.[4] 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.

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. Hub functions will include facilitating the access to 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.[5]

To determine CMS's progress in implementing security requirements for the Hub, OIG reviewed documentation, project schedules, and timelines; interviewed CMS employees and contractors and personnel from key Federal agencies working with CMS during development of the Hub; and reviewed CMS's security testing results.

[3] 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).

[4] 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. For the purposes of this report, "exchanges" refers to all three types of health insurance exchanges.

[5] 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.*

Results of OIG's Review

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. The following observations provided the status of CMS's implementation related to security controls, security testing, and coordination at the time of our fieldwork.

Security Authorization

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. At CMS, the authorizing official is the Chief Information Officer (CIO).

The security authorization package must include a system security plan, information security risk assessment, and security control assessment 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. Under the NIST guidelines, 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.

At the time of our review, the security authorization decision by the CMS CIO was expected by September 30, 2013. Since our review, CMS has reported that the security authorization was obtained on September 6, 2013.

System Security Plan and Information Security Risk Assessment

CMS incorporated the elements required for adequate security into the draft Hub system security plan. The plan (1) provides an overview of the security requirements of the system, (2) describes the controls in place or planned (e.g., access controls, identification and authentication) for meeting those requirements, and (3) delineates the responsibilities and behavior expected of all individuals who access the system.

CMS was still drafting the information security risk assessment at the time of our review. For this reason, we could not assess CMS's efforts to identify security controls and system risks and implement safeguards and controls to mitigate identified risks. Key aspects of the assessment 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.

At the time of our review, the CMS contractor did not expect to be able to provide finalized security documents, including the system security plan and risk assessment, to CMS for its review until July 15, 2013. Since our review, CMS reported to us that the documents were provided to CMS on July 16, 2013.

Security Control Assessment and Testing

At the time of our review, CMS and its contractors were performing security testing throughout the Hub's development, including vulnerability assessments of Hub services. CMS was logging and tracking defects and vulnerabilities, as well as correcting and retesting Hub services to ensure that vulnerabilities are remediated.

A security control assessment of the Hub must be performed by an independent testing organization before the security authorization is granted.[6] The assessment 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 security control assessment test plan is to explain clearly the information the testing organization expects to obtain prior to the assessment, the areas that will be examined, and the activities expected to be performed during the assessment.

According to CMS, the assessment was scheduled to be performed between August 5 and 16, 2013. Since the assessment was not completed at the time of our review, we could not determine whether vulnerabilities identified by the testing would be mitigated. Since our review, CMS has reported to us that the assessment was completed on August 23, 2013.

Adjustments to CMS Timelines

CMS provided us with timelines in March 2013 and May 2013 for its system security plan, risk assessment, security control assessment, and security authorization decisions. CMS also provided us additional information on timing of certain steps after the May timeline. Some key targets had been moved to later dates as the development of the Hub was continuing. It is important to note that these were internal target dates set by CMS for these milestones and not mandated deadlines.

For example, in March, the security control assessment test plan was targeted to be provided to CMS on May 13, 2013, and this due date was subsequently moved to July 15, 2013, and the start date of the security control assessment was moved from June 3, 2013, to August 5, 2013. CMS stated that the security control assessment timeframe was moved so that performance stress testing of the Hub could be finished before the assessment and any vulnerabilities identified during the stress testing could be remediated. Otherwise, CMS might need to perform an additional assessment after the remediation was complete.

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

According to CMS's timeline from May 2013, the security authorization decision by the CMS CIO was expected on September 30, 2013. OIG noted in our report that if there were 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 open enrollment period set to begin on October 1, 2013. In its comments on our draft report, CMS stated that it was confident that the Hub would be operationally secure and it would have a security authorization before October 1, 2013.

Since our review, CMS has reported to us that the security authorization was obtained on September 6, 2013.

Coordination Between CMS and Its Federal and State Partners

Our review observed that CMS was 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. CMS developed an approach for interagency testing and has developed test plans. At the time of our review, CMS was in the process of executing its test plans, which included testing for secure communications between CMS and its Federal and State partners and performance stress testing of the Hub. In addition, CMS has developed security-related documents and security agreements regarding Federal information systems and networks. 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 has 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 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 developing the ICDs and signed the ICDs in May 2013.

Federal policy requires agencies to develop Interconnection Security Agreements (ISAs) for Federal information systems and networks that share or exchange information with external information systems and networks.[7] The Master ISA describes the systems' environment; the 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 for maintaining the security of ACA systems.

[7] 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.

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, which will be signed by the Federal partner authorized official. Since our review, CMS has reported to us that all ISAs with its Federal partners are expected to be approved by September 27, 2013.

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 was expected to be signed by July 26, 2013; and the SLA with SSA was expected to be signed by September 27, 2013. The SLAs with the remaining Federal partners (VHA, DoD, OPM, and Peace Corps) were expected to be signed by September 20, 2013. Since our review, CMS has reported to us that the SLAs with IRS, VHA, and DHS are expected to be signed before the end of September. CMS also reported that DoD-Tricare and CMS have agreed to allow transactions to occur and monitor the "response time metric" to set a baseline for the interaction standards before they execute their SLA. They expect to execute their SLA by the end of December.

Concluding Observations

CMS is taking steps to ensure that there are adequate security measures for the Hub in compliance with NIST guidelines At the time of our review, CMS was working with very tight deadlines to ensure that security measures for the Hub were assessed, tested, and implemented by the expected initial open enrollment date of October 1, 2013.

Our report provided the status of the implementation of key security requirements at a point in time. CMS has reported to us that it has completed all of the required steps and obtained its security authorization on September 6, 2013. We have not independently verified CMS's progress since completing our audit.

Thank you for your interest in our work on this important issue and the opportunity to be a part of this discussion. I would be pleased to answer your questions.