U.S. House Committee on Energy & Commerce Subcommittee on Health
Hearing on "PPACA Pulse Check: Part 2"
Supplemental Written Testimony of Michael Finkel
Quality Software Services, Inc.
October 10, 2013

Supplemental Responses to Member Questions

The Honorable Joseph R. Pitts' Questions

Q: Will you please elaborate on the security systems that will protect data in the hub you are creating?

A: Under the Federal Information Security and Management Act, CMS is required to follow the National Institute of Standards and Technology's security standards and guidelines for federal IT systems. As a system integrator, QSSI was responsible for assuring that the design and development of the Data Services Hub complied with these NIST standards. QSSI has met its obligations from a system design and development standpoint.

As I mentioned in my testimony, the Data Services Hub code is being developed, will launch, and will operate from within the CMS secure cloud hosted at the Terremark Data Center. Once in production, CMS will enforce additional security controls to protect the system, including controlling access and changes to the system. The Data Services Hub will be monitored continually by CMS and its information security contractors.

While QSSI does not have full visibility into all of the layers of security CMS has in place, CMS has announced that the Data Service Hub and the associated component systems that comprise the health insurance market place (other than the State-Based Marketplaces) have several layers of protection in place to mitigate information security risk. For example, these systems will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action against irregular behavior and unauthorized system changes that could indicate a potential incident. If a security incident occurs, CMS has noted that its Incident Response capability would be activated, which allows for the tracking, investigation, and reporting of incidents. This allows CMS and the Department of Health and Human Services (HHS) to quickly identify security incidents and ensure that the relevant law enforcement authorities, such as the HHS Office of Inspector General Cyber Crimes Unit, are notified for purposes of possible criminal investigation.

Q: Has QSSI completed stress testing of their system? Will you describe what stress testing entails and when you expect such stress testing to be complete?

A: QSSI has completed its stress testing of the Data Service Hub. Based on that testing, QSSI believes that the Data Services Hub will be able to transmit the necessary number of queries.

The Honorable Gus Bilirakis' Questions

Q: In your statement, you mention that a security risk assessment by a contractor did not identify any issues that would prevent the data services hub from launching. Did the security assessment find any security concerns? Will you provide this committee with a copy of that report?

A: The Security Risk Assessment did not find any issues that would preclude authorization to operate. As is common, the Security Risk Assessment identified a number of areas for enhancement. For example, the Security Risk Assessment proposed documentation enhancements and password setting protocol enhancement. QSSI has either addressed the recommendations or, in the case of a few non-critical items, identified enhancements that are pending approval or completion. The Mitre Corporation provided the final version of the Security Risk Assessment to CMS, and QSSI does not have a copy currently.

Q: According to the Inspector General's report, it says that CMS's Chief Information Officer is expected to make his Security Authorization on September 30, one day before the Exchanges go online. Is it responsible to make this decision so late in the process? The original timeline was for it to be made on September 4.

A: As noted in our testimony, an independent third-party tester, the Mitre Corporation conducted an independent Security Risk Assessment of the Data Services Hub which was completed on August 30, 2013. The Mitre Corporation provided its Security Risk Assessment to the CMS Chief Information Officer to allow him to assess whether or not to authorize operation of the Data Services Hub by CMS.

Based on the Mitre Corporation Security Risk Assessment, the CMS Chief Information Officer provided the security authorization on September 6, 2013, well in advance of October 1.

Q: According to the Inspector General's report, the final report for the Security Control Assessment (SCA) is not due until September 20. That gives CMS 10 days to review the report and make any changes to your system. Is that really adequate time for CMS to do this? How much time would you have in the commercial sector?

A: As noted above, the Security Risk Assessment was completed on August 30, 2013, and the security authorization was signed on September 6, 2013, well in advance of October 1. In

our experience, the timing of assessments depends on numerous variables. The timing of the assessment and the authorization is not notable based on QSSI's past experience in prior projects.

Q: Has HHS, CMS, or another government agency come back to you and asked you to modify the initial contract? Is so, what was changed? Did CMS state why they needed to make this change or why this was not included in the original bid?

A: As is common, CMS has issued contract modifications since the original Data Services Hub contract was awarded. Among other things, the modifications provided for the development of an Electronic Data Interchange which will be used to translate files from the federal and state marketplaces into a format that is more readily processed by issuers. As with the Data Services Hub, the Electronic Data Interchange is housed at the Terremark Data Center and operated by CMS. Other aspects of the modifications included the provision of additional hardware and software, as well as infrastructure support for CMS to operate its operations center.

Q: What security standards do you use? Do you use FISMA standards for your private contracts? How would FISMA standards compare to the equivalent security standards? Would you describe it as a higher or lower standard?

A: As noted in our testimony, as a CMS system, the Data Services Hub is covered by the Federal Information Security and Management Act and the security requirements set forth therein. Federal Information Security and Management Act was signed into law in 2002 and has been subsequently amended. Systems that are developed for private parties do not typically need to conform to the security requirements set forth in the Federal Information Security and Management Act. Commercial standards are often developed based on the Federal Information Security and Management Act standards.

<u>The Honorable John Dingell's Requests</u>

Q: Some have argued that the data hub will be a new government database with personal medical information. Is this an accurate characterization of the program? If not, what is the correct representation of the circumstances?

A: No, it is not an accurate characterization. The Data Services Hub is a tool that will transfer data. The Hub's function will be to move data, acting as a router of data between a given marketplace and various data sources.

The Data Services Hub will route data that will be used by the health insurance marketplaces to verify applicant information data to determine eligibility for qualified health plans and insurance programs, as well as for Medicaid and CHIP. A consumer interested in purchasing health insurance online will go to a health insurance marketplace's web portal to fill out

enrollment forms and select a plan. Certain information the consumer provides to the marketplace, such as citizenship, will have to be verified. The marketplace will direct a query to external information sources, such as government databases, through the Data Services Hub. The Data Services Hub will not store the verification data or the content of the queries made by the marketplaces.

Once the requested verification information is sent back to the marketplace, eligible consumers are then able to enroll in one of the available plans. The Data Services Hub will not determine consumer eligibility, nor will it determine which health plans are available in the marketplaces. The enrollment data, such as name, address, and premium amount, will then be transferred through the Data Services Hub from the originating marketplace to the health plan the consumer chooses.

While the Data Services Hub will pass eligibility data from verification sources to the federal and state marketplaces, and enrollment data from marketplaces to plan issuers, it will not handle any personal medical records.

CMS owns and will operate the Hub, which is housed in the CMS secure cloud hosted at the Terremark Data Center.

Q: Would you please provide a summary of the functions of the data hub?

A: The principal functions of the Data Services Hub are the following services provided to the Federally-Facilitated Marketplace and the State-Based Marketplaces (collectively "marketplaces"):

- Eligibility Verification Support:
    - The Data Services Hub will transmit verification requests from health insurance marketplaces to trusted databases, such as databases operated by the Social Security Administration, the Internal Revenue Service, the Department of Homeland Security, the Department of Veterans Affairs, Medicare, TRICARE, and Equifax. The Data Service Hub will then transmit the responses from the relevant database back to the originating marketplace.
    - For State-Based Marketplaces, the Data Services Hub will transmit an identity verification request to Experian. The Data Services Hub will then transmit the response from Experian to the originating marketplace.
    - The data transmitted will pertain to the applicant's identity and enrollment information, but will not include personal medical information.
    - The marketplaces, not the Data Services Hub, will serve as the "front door" for consumers to fill out an online health insurance application and to review qualified plans.
    - The Data Services Hub does not make eligibility determinations, which is a function of the marketplaces.

- The Data Services Hub does not store the content of the verification requests or the responses from the trusted sources.

- Enrollment Support:
  - The Data Services Hub will transmit enrollment data from the Federally-Facilitated Marketplace to issuers. The Data Services Hub will then transmit an acknowledgement from the issuer to the Federally-Facilitated Marketplace.
  - The Data Services Hub does not make enrollment selections, which are made by the applicant.
  - The Data Services Hub does not store the content of the qualified plans or the enrollment data.

- Plan Management Support:
  - The Data Services Hub will transmit information about qualified health insurance plans from issuers to the Federally-Facilitated Marketplace. The Data Services Hub does not make plan qualification determinations.
  - The Federally-Facilitated Marketplace is the tool that CMS will use to certify and manage qualified plans.

- Financial Management Support:
  - The Data Services Hub will transmit a list of issuers from the Federally-Facilitated Marketplace to the CMS accounting system for purposes of premium amounts.
  - The Data Services Hub does not determine reinsurance payments, risk adjustments and corridors, or premium amounts. The Federally-Facilitated Marketplace is the tool that CMS will use to calculate reinsurance payments, risk adjustments and corridors, and premium amounts.