Henry Chao’s Hearing
“HealthCare.gov”
Energy & Commerce Committee
Oversight & Investigations Subcommittee

November 19, 2013

Attachment 1—Additional Questions for the Record

The Honorable Cory Gardner

1. Was there any consultation or recommendations from CMS to states on how to develop their websites?

Answer: Section 1311 outlines Federal requirements for Marketplaces. These include the minimum functions the Marketplace must undertake as well as the oversight responsibilities the Marketplace must exercise in certifying and monitoring the performance of qualified health plans. Plans participating in the Marketplace must also comply with state insurance laws and Federal requirements in the Public Health Service Act. In defining the authority and duties of a Marketplace, states were required to incorporate, by reference or explicit provisions, the Federally-required Marketplace functions and oversight responsibilities as required by section 1321 of the Affordable Care Act.

2. Do you know the extent of the interaction between CMS and Connect for Health Colorado?

Answer: CMS is working with all states to continually improve their systems and business processes in accordance with published regulations and guidance. The foundation of the seamless consumer experience between state-based Marketplaces and Medicaid and CHIP agencies is formed through the development and use of a shared single eligibility system.

3. To the best of your knowledge, have state websites been tested? If so, are they safe for the consumer?

Answer: Yes, as part of each state’s Blueprint submission, states had to both attest to, and submit test files to and receive files from the Data Services Hub. These included IT tests for functionality and compliance to established IT requirements. Tests included verification of compatible technology, infrastructure, and bandwidth required to support all Marketplace activities, as well as verification of a secure connection between the state system and the Data Services Hub. Tests were reviewed and confirmed to be effectively implemented by the independent verification and validation (IV&V) team through quality management processes and test procedures for Marketplace-development activities. Testing included verification of a secure connection between the state system and the Data Services Hub. A senior official in each state attested to their adherence to, and compliance with, the established security and privacy framework.

4. **Were states able to utilize CMS' contractors to test their websites?**

Answer: Each state-based Marketplace had its own vendor selection and IT development process separate from the contracting and IT development for the Federally-facilitated Marketplace.

5. **Is Connect for Health Colorado fully functional?**

Answer: Coloradans interested in what insurance options are available to them can browse plans directly through Connect for Health Colorado – Colorado's State-based Marketplace – If Coloradans are seeking financial assistance, they can apply in a coordinated, integrated application process that will result in an eligibility determination for any of the three affordability programs (advanced payment of the premium tax credits/cost sharing reductions, Medicaid or CHIP).

6. **Has end-to-end testing been completed for state-run exchange websites?**

Answer: As noted above, each state was required, as part of its Blueprint submission, to have a plan for testing their website, including the site's functionality. Marketplaces also must have capacity to accept and process applications online, compute APTCs, and process QHP selections and terminations electronically in coordination with issuers and CMS, among other Marketplace functions.

7. **How has the connection between the state exchange and other databases, including federal databases, been tested for security and privacy?**

Answer: In keeping with industry practice, CMS established strong security controls and standards, which each state was required to meet in order to connect to the Hub. These controls and standards are based on the guidelines issued by the National Institutes of Standards and Technology (NIST). Each state is required to establish a secure socket layer (SSL) connection between the state system and the Data Services Hub, to include FIPS 140-2 compliant encryption algorithms.

8. **Are you confident the state sites do not present a risk?**

Answer: States are required to meet the Blueprint requirements, pass functional and security testing, and sign a number of agreements attesting to the readiness and security of their IT system. Each state that was connected to the Hub on October 1 had either completed an authority to connect (ATC), or was granted a short-term ATC. Before an ATC is issued, states must sign a Computer Matching Agreement, an Interconnection Security Agreement and an Information Exchange Agreement, all of which bind the state to rules and operating procedures related to data security and privacy. Additionally, states are required to complete a security plan, a risk assessment, a corrective action plan to address risks, and a self-assessment or a third party test for each security control. Every state that was connected on October 1 adhered to these procedures.

The Honorable G.K. Butterfield

1. **The Hub and Marketplace systems have robust security systems designed to enable CMS to remain vigilant against any security threat.**

   a. **Can you provide some examples of instances which would cause CMS to take a closer look at a potential incident?**

Answer: Any unusual activity would cause CMS to examine an incident more closely.

   b. **Who would make the determination whether to initiate the Incident Response capability?**

Answer: The Incident Response (IR) process is activated every time an internal alert or external report of an event is triggered. The IR process includes the early workflow to triage all events and to place them into threat categories. Appropriate response processes are established for each threat category.

   c. **Would law enforcement authorities be notified automatically and in real time if the Incident Response capability was activated?**

Answer: If a violation of the law is suspected, the CMS security team notifies the Chief Information Security Officer of HHS, who in turn notifies the Office of Inspector General (OIG) Computer Crime Unit and also submits a report to the United States Computer Emergency Readiness Team (US CERT). Within CMS and HHS, the notification processes to these entities are automated to allow for rapid notification and response.

2. **Mr. Chao, you indicated that the issues that have delayed many of the 137,000 individuals in my district who are anxious to sign up for the ACA were due to an underestimation of the volume of users and in no way connected with security delays. It seems apparent that strong security safeguards are in place and that once the website is up and running our constituents can use it with confidence.**

   a. **With the Hub up and running as intended, can you explain why eastern North Carolinians should feel safe using it and what added efficiency and security benefits it provides?**

Answer: The security and protection of personal and financial information is a top priority for CMS, which, for decades, has protected the personal information Americans enrolled in Medicare, Medicaid, and CHIP. CMS used this experience and our security best practices to build a secure Data Services Hub that consumers should feel confident using.

CMS follows Federal law, government-wide security processes, and standard business practices to ensure stringent security and privacy protections. CMS' security protections are not singular in nature; rather the marketplace is protected by a vast array of security layers. First, the system was developed with secure code. Second, the system's infrastructure is physically and logically protected by our hosting provider. Third, the system is protected through an internet defense shield in order to minimize access to any personal data. Finally, several entities provide direct and indirect security monitoring, security testing, and security oversight which include various organizational groups in CMS, HHS, US-CERT at the Department of Homeland Security (DHS), and the HHS OIG. Each of these groups have varying roles to ensure operational, management, and technical controls are implemented and successfully working. The Data Services Hub is protected by the high standards demanded of Federal information systems, including the standards prescribed by FISMA, NIST, the Privacy Act, and the Office of Management and Budget (OMB).

A large number of connections can cause security vulnerabilities. The Hub allows for one highly secured connection between closed databases of trusted states and Federal agencies instead of hundreds of connections. A series of business agreements enforce privacy controls between CMS and our Federal and state partners.

b. As the Marketplace interface comes online, can you discuss some of the security benefits that site provides to consumers, including the fact that they no longer need to provide detailed medical history?

Answer: HealthCare.gov does not collect personal health information (PHI). PHI is not necessary to the single streamlined application process because, due to the guaranteed issue provision of the Affordable Care Act, issuers are prohibited from denying applicants insurance based on their pre-existing conditions. Therefore, consumers in the Marketplace do not need to disclose details of their medical history as they might have had to do when they applied for health coverage in the past. Additionally, CMS follows Federal law, government-wide security processes, and standard business practices to ensure stringent security and privacy protections for the limited personal information provided in the single, streamlined application.

3. Both the data services Hub and the Federally-facilitated Marketplace eligibility and enrollment system build on existing information technology systems.

a. Can you explain how the Hub and Marketplace systems build on the security systems from programs like Medicare Advantage and State Medicaid agencies?

Answer: The Hub and Marketplace systems have the same stringent security standards that CMS has employed to protect other databases and information. CMS developed the Marketplace systems consistent with Federal statutes, guidelines and industry standards that ensure the security, privacy, and integrity of systems and the data that flows through them. All of CMS' systems of records are subject to the Privacy Act of 1974, the Computer Security Act of 1987, and the Federal Information Security Management Act of 2002. These systems must also comply with various rules, regulations, and standards promulgated by HHS, OMB, DHS, and NIST.

4. It is clear that many existing laws, rules, regulations, and standards have been met for the Hub and Marketplace systems to operate. In other words, keeping sensitive information secure at HHS seems to be something your agency does in other areas.

a. **Your agency has demonstrated before that it is able to effectively safeguard sensitive personal information from individuals, is that correct?**

Answer: CMS has worked diligently over many years to protect the sensitive information we are tasked with maintaining as part of our services to millions of Americans. CMS operates and oversees systems that contain sensitive information about Medicare beneficiaries, physicians who participate in Medicare, and Medicare claims.

b. **Can you provide example where HHS has managed an information technology system and protected sensitive personal information and compare that system to the Hub and Marketplace?**

Answer: The Medicare program utilizes CMS' information systems to protect sensitive information about the Medicare beneficiaries, physicians who participate in Medicare, and Medicare claims. While the Hub and Marketplace serve a different population, our commitment to protect the private information of consumers, providers, and beneficiaries remains the same.

The Hub provides one highly secured connection among trusted Federal and state agencies instead of requiring each agency to set up what could have amounted to hundreds of independently established connections. Further, the Hub is not a database; it does not retain or store information. It is a routing tool that can validate applicant information from various trusted Government agencies through secure networks.

Attachment 2—Member Requests for the Record

During the hearing, Members asked you to provide additional information for the record, and you indicated that you would provide that information. For your convenience, descriptions of the requested information are provided below.

The Honorable Michael C. Burgess

1. **Do you feel during your time that there has been a single implementation leader that you could look to for advice and direction throughout this process? If so, please provide their name(s).**

Answer: As Administrator of CMS, Marilyn Tavenner oversees Affordable Care Act implementation.

The Honorable Gregg Harper

1. **Do you have a central reporting location of the navigators that are in violation or reported in violation?**

Answer: The Navigator program and grantees are overseen by the Center for Consumer Information and Insurance Oversight and by the Office of Acquisition and Grants Management, which ensure that all grantees abide by the terms of their funding agreements.

CMS has several tools to respond to any organizations found in violation of the terms of the Federal Navigator program, including issuing a Corrective Action Plan to the grantee, decertifying individual Navigators, and terminating the grant.