THE COMMITTEE ON ENERGY AND COMMERCE

MEMORANDUM

November 17, 2013

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on “Security of HealthCare.gov”

On Tuesday, November 19, 2013, at 10:15 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled “Security of HealthCare.gov.” This hearing will focus on the issues surrounding the implementation of the Patient Protection and Affordable Care Act’s (PPACA) health insurance exchanges and the security of HealthCare.gov.

I. WITNESSES

The following witnesses will testify at the hearing:

Panel I:

Mr. Henry Chao
Deputy Chief Information Officer and Deputy Director of the Office of Information Services
Centers for Medicare and Medicaid Services (CMS)

Panel II:

Mr. David Amsler
President and Chief Information Officer
Foreground Security, Inc.

Ms. Maggie Bauer
Senior Vice President, Health Services
Creative Computing Solutions, Inc. (CCSi)

Mr. Jason Providakes
Senior Vice President and General Manager
Center for Connected Government
MITRE Corporation (MITRE)

The Committee invited Verizon Terremark Federal (Verizon Terremark) to testify at the hearing. Verizon Terremark informed the Committee on November 16, 2013, that it declined the Committee's invitation to testify.

II. BACKGROUND

Over the last year, the Committee has asked Administration witnesses about the status of HealthCare.gov and whether the administration was ready for the launch of open enrollment on October 1, 2013. For example, in her testimony to the Committee on August 1, 2013, CMS Administrator Marilyn Tavenner assured the Committee that "CMS has been conducting systems tests since October 2012 and will complete end-to-end testing before open enrollment begins."

After the failed October 1 launch, the Committee opened an investigation into the implementation of the PPACA and the failed launch of the HealthCare.gov website. On October 10, 2013, the Committee sent letters requesting documents and certain information from the U.S. Department of Health and Human Services (HHS), CGI Federal, and Quality Software Services, Inc. (QSSI). After the Committee received documents indicating that the failure to conduct end-to-end testing prior to the October 1 launch presented certain security risks, the Committee sent letters on October 31, 2013, to HHS, MITRE, Verizon Terremark, CCSi, and Foreground requesting certain documents and information relating to the security of the Federally Facilitated Marketplace (FFM).

In response to these letters, the Committee has received initial document productions and Committee staff briefings from CMS officials and contractors. The Committee's investigation of the failed launch of HealthCare.gov is ongoing. Part II(A) of this memorandum provides background on the security-related aspects of Federal information technology systems development. Part II(B) provides a summary based on the documents and briefings provided to date to the Committee of how FFM applications and HealthCare.gov were tested for security and CMS' management of this process.

A. Overview of the Development of the Federally Facilitated Marketplace

PPACA implementation has involved multiple government agencies and contractors. Agencies such as the CMS, Internal Revenue Service, Social Security Administration, U.S. Department of Homeland Security, and the Office of Personnel Management are involved in the implementation of the PPACA exchanges. In addition, the HHS has entered into contracts with organizations to assist with the creation and operation of such exchanges, including the FFM. These contractors also are tasked with developing the applications that integrate the various components of the FFM.

Several contractors and various government officials play a role in the security of HealthCare.gov. The FFM is comprised of government agencies, user applications, data centers and State marketplaces. Each piece of the FFM infrastructure requires that security be imbedded into the framework.[1] Ideally, functionality of the system complements the security, and the security is tested and improves as the system matures.[2]

Federally owned and operated IT systems must comply with several security standards. The Federal Information Security Management Act of 2002 (FISMA) outlines the basic requirements or framework for managing information security. Additionally, Federal IT systems must meet certain baseline security requirements. Agencies develop these baseline security requirements by establishing appropriate security controls and assurance requirements. Agencies have flexibility in applying the baseline security controls depending on the type of IT systems they manage.[3] Agencies, therefore, must customize the security controls to optimize mission requirements within the IT environment.[4]

Once security baselines or security controls have been developed and tailored to the needs of the IT system, the application developers and IT network service providers can integrate the security baselines into the overall system. Once the individual applications are developed, they are subject to a stress test known as a Security Control Assessment (SCA). The purpose of the security assessments is to identify security deficiencies and validate whether the application properly embeds the security controls.[5] These assessments may result in the recommendation of additional controls. Once a deficiency is identified, a finding is made and a level of risk is assigned to the finding. Additionally, if deficiencies are identified, they are mitigated if possible or a schedule is established in which the deficiencies are remediated.

After the assessments are completed and the systems and applications are integrated into the IT network, additional security measures ensure that the IT systems protections remain robust. Several examples of these measures include continuous monitoring, configuration management, systems access controls, and detection capabilities.

During the course of the Committee’s investigation of the implementation of the PPACA, the Committee has identified several contractors that work with CMS to develop and validate the security controls and monitor system traffics with various tools and procedures. The following is a description of the security-related work performed by the FFM contractors who will testify at the November 19 hearing:

- MITRE was awarded a contract by CMS in November 2012. Under this contract, MITRE developed a Federal Facilitated Research and Develop Center (FFRDC) within CMS. One of the roles of the FFRDC was to develop the security control baselines for the exchanges. After MITRE developed these security controls, CMS disseminated the security controls to the contractors creating the applications for the FFM, which included CGI and QSSI. The contractors that developed the applications for HealthCare.gov were responsible for

[1] See generally, NIST Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004.
[2] See generally, NIST Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 2013.
[3] Special Publication 800-53, Rev. 4, Section 1.4 Organizational Responsibilities. p. 4.
[4] Special Publication 800-53, Rev. 4, Section 1.4 Organizational Responsibilities. p. 4-5.
[5] NIST Special Publication 800-30, Rev. 1, 2012, provides guidance on the risk assessment process.

incorporating the security controls into the design of the applications. Once the applications were close to completion, MITRE performed the SCAs. The timing and the scope of the SCAs were determined by CMS. These SCAs test the applications' integration of the security baselines. Over the course of 2013, MITRE conducted four SCAs of FFM applications. For the FFM, the Enterprise Information Security Group (EISG) within the Office of Information Services (OIS) at CMS worked with MITRE to develop the risk assessments and oversees that they are conducted correctly.

- Verizon Terremark provides CMS with managed infrastructure services for the Federal Data Services Hub (DSH). Verizon Terremark was awarded its contract with CMS in November 2012. That contract will expire in March 2014. In this capacity, Verizon Terremark provides a quasi-private cloud computing environment which consists of hosting IT hardware within a virtualized network infrastructure housed in a large data center. The operating systems for the network infrastructure have security embedded in the physical architecture of their system. The applications developed by other contractors are then hosted on this infrastructure at the data center. CMS informed Committee staff that Verizon Terremark also provides external intrusion detection and perimeter security for the DSH.

- CCSi and Foreground Security monitor the perimeter firewalls and network devices for the eCloud. In August 2012, CCSi was awarded a small business contract, and Foreground Security is their subcontractor under the contract. In addition, these companies are responsible for scanning the code of the various applications in order to identify any security vulnerabilities. CCSi and Foreground Security are required to report any incidents they identify directly to CMS for remediation. They are also responsible for configuring CMS-furnished equipment within the Verizon Terremark eCloud.

Within CMS, responsibility for security is divided between two offices. Security related issues with the software applications, or those applications that users interact with on the exchanges and in the FFM, are managed by the Consumer Information and Insurance Systems Group, Marketplace Security Group (MSG) at CMS. The MSG oversees the remediation of security configuration flaws and vulnerabilities in the network infrastructure and the business applications. This group is headed by Monique Outerbridge, who reports directly to Deputy Chief Information Officer (CIO) Henry Chao. The other office responsible for security, EISG, establishes the security baselines and oversees the performance of the SCAs. The EISG is headed by Theresa Fryer. CMS Chief Information Officer Tony Trenkle worked closely with the personnel in EISG to develop the security baselines and conduct the SCAs. Mr. Trenkle's last day with the agency was November 15, 2013.

B. The Committee's Investigation of the Security of HealthCare.gov

Contracts for the design and development of two of the primary applications of HealthCare.gov – CGI and QSSI – were awarded by CMS in the fall of 2011. Approximately one year later, CMS awarded contracts to MITRE, CSSi, Foreground, and Verizon Terremark to develop other components of the FFM, including those related to security.

Beginning in January 2013, MITRE conducted a SCA of the Enterprise Identity Management (EIDM) application developed by QSSI. This SCA was completed on February 13, 2013. According to the SCA report drafted by MITRE, several high risks were identified and all were mitigated. The SCA also stated that as the EIDM was due for a new release, which added "significant functionality" and required a new SCA to be performed, "MITRE strongly recommends that CMS perform a comprehensive SCA of all subsequent releases of [the] EIDM . . . ."[6] Documents produced to the Committee to date do not indicate whether MITRE's recommendation to perform SCAs on subsequent releases of the EIDM was followed.

In June 2013, pursuant to its contract, MITRE conducted an SCA of the Exchange Consumer Web Services (ECWS) developed by Aquilent. According to MITRE's report issued on August 23, 2013, "[d]uring and after the assessment, Aquilent technicians focused their efforts on remediating the findings, with an emphasis on closing High and Moderate risk-level findings."[7]

In August 2013, MITRE conducted a SCA of the DSH. A MITRE report issued on this SCA on October 4, 2013, stated that MITRE identified several high risk findings and recommended that "[w]hile all findings will need to be addressed, findings representing a high risk to CMS data should be addressed first and closed or mitigating controls implemented to reduce the risk exposure to CMS."[8] The DSH received its Authorization-to-Operate (ATO) from CMS on September 6, 2013.

The final SCA before the October 1 start of open enrollment began in August 2013 and was completed on September 19, 2013. During this SCA, MITRE examined the Health Insurance eXchange (HIX) developed by CGI Federal. MITRE informed Committee staff during a briefing that CMS had to modify the scope of this assessment by limiting the systems and applications to be tested, because several of them were not complete. In its final report on this SCA, issued October 11, 2013, MITRE concluded that it was "unable to adequately test the Confidentiality and Integrity of the HIX system in full."[9] MITRE explained that, for purposes of the SCA, it was supposed to examine the "potential security risks to CMS" regarding applications and modules "not tested previously." MITRE went on to note that "[c]omplete end to end testing of the HIX application never occurred." Additionally, MITRE indicated in its report that at the time of the August-September SCA of the CGI HIX, several applications were still "being developed" and "impacted end to end MITRE test cases."[10]

The findings of MITRE's SCAs of the DSH and CGI's HIX necessitated that CMS issue certain authorizations prior to the October 1, 2013, launch of HealthCare.gov. On September 3, 2013, CMS CIO Trenkle issued an Authorization Decision for the FFM Qualified Health Plans and Dental modules. In this decision, the CIO determined that, based on the findings in the earlier SCA, "the risk to CMS information and information systems resulting from the operation of the

[6] CMS Enterprise Identity Management Security Control Assessment (SCA) Report, April 5, 2013.
[7] CMS Exchange Consumer Web Service (ECWS) Security Control Assessment (SCA) Report, August 23, 2013.
[8] CMS Federal Data Services Hub (DSH) Security Control Assessment (SCA) Report, October 4, 2013.
[9] CMS Health Insurance eXchange (HIX) August-September 2013, Security Control Assessment (SCA) Report, October 11, 2013.
[10] CMS Health Insurance eXchange (HIX) August-September 2013, Security Control Assessment (SCA) Report, October 11, 2013.

FFM information system is acceptable."[11] The decision to accept the risks for the site to operate was predicated on a list of mitigation measures that were to be completed in the future. The ATO listed the specific security findings and the schedule for mitigating those risks: five were to be completed in 2014, and the sixth in 2015.

As discussed earlier, the SCA conducted by MITRE of the CGI HIX in August and September revealed that no end-to-end testing was conducted prior to the beginning of open enrollment. During a briefing with Committee staff, CMS CIO Trenkle stated that given the high profile of the FFM and the risks associated with launching on October 1, 2013, it was his recommendation that CMS Administrator Tavenner sign an ATO after he informed her of the risks to the FFM. CMS CIO Trenkle also signed a separate Decision Memorandum that stated the mitigation plan that was in place because of these risks "does not reduce the risk to the FFM system itself going into operation on October 1, 2013."[12] In a separate briefing with Committee staff, Deputy CIO Chao explained that while he edited this memorandum, he was not familiar with the specific risks discussed in the memorandum because he had not seen the results of the SCA outlining the inability to test the system from end-to-end in a single environment.

On the recommendation of CMS CIO Trenkle, on September 27, 2013, CMS Administrator Tavenner signed a memorandum acknowledging that the FISMA required that the FFM "successfully undergo a Security Control Assessment (SCA)" and that "[d]ue to system readiness issues, the SCA was only partly completed." According to this memorandum, "[f]rom a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for the FFM." By signing this memorandum, CMS Administrator Tavenner recommended that CMS issue an "Authority-to-Operate" for six months that would allow the FFM to go forward with a mitigation plan in place and to perform a "complete SCA."

III. ISSUES

The following issues will be examined at the hearing:

- CMS' management of the security of the FFM and the roles and responsibilities of the various contractors for the security of the FFM;
- How the failure to perform complete end-to-end testing prior to the October 1, 2013, launch of HealthCare.gov affects the security of the FFM;
- CMS' current assessment of the security of HealthCare.gov and whether vulnerabilities have been identified.

IV. STAFF CONTACTS

[11] Authorization Decision for the Federal Facilitated Marketplaces (FFM) System, from Director of OIS, September 3, 2013.

[12] "Federal Facilitated Marketplace Decision Memo Risk Acknowledgment Signature Page," signed: T. Fryer, T. Trenkle, M. Snyder, dated: September, 27, 2013.

If you have any questions regarding this hearing, please contact Karen Christian, Carl Anderson, or Sean Hayes of the Committee staff at (202) 225-2927.