HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
STATEMENT OF THE MITRE CORPORATION
November 19, 2013

Good morning Chairman Murphy, Ranking Member DeGette and distinguished members of the committee. My name is Jason Providakes and I am here today on behalf of The MITRE Corporation. I serve as the director of the not for profit Federally Funded Research and Development Center (FFRDC), operated by MITRE and sponsored by the U.S. Department of Health and Human Services.

The MITRE Corporation is chartered in the public interest to apply systems engineering skills and advanced technology to address issues of critical national importance. We accomplish this through the operation of research and development centers that support our government sponsors with scientific research and development, analysis, and systems engineering and integration. Known as Federally Funded Research and Development Centers, they are operated under a set of rules and constraints prescribed by the Federal Acquisition Regulations (FAR). The rules are designed to preserve the FFRDC's objectivity, independence and freedom from conflict of interest.

MITRE operates FFRDC centers for seven federal agency sponsors. We were awarded the contract to operate the CMS Alliance to Modernize Healthcare center about a year ago, following a competitive bid process. The center is charged with assisting CMS in modernizing its operations and supporting the implementation of health reform and expansion of health care to millions of Americans.

MITRE serves as a technical independent, objective advisor to CMS/HHS. We have been supporting CMS/HHS successfully since 2005 on a contract basis prior to the establishment of the new center. We advise on Health IT; help plan and develop future policies; provide technical evaluation and objective evaluation of business models; and assess new technology.

As part of its efforts to establish HealthCare.gov, CMS asked MITRE to conduct security assessments on parts of the site. I appreciate this opportunity to clarify what our role was in assisting CMS on HealthCare.gov.

We provide CMS with information security support and guidance under two contracts with the Office of Information Systems (OIS), Enterprise Information Security Group (EISG). Pursuant to tasking issued under those contracts, MITRE performed a total of 18 Security Control Assessments, or SCAs, for components across a range of CMS enterprise systems. Most of these were performed on supporting infrastructure (utilities) and development components. Six of the SCAs were directly related to HealthCare.gov and were performed between September 17, 2012 and September 20, 2013.

MITRE performs various tasks as part of our overall support for CMS enterprise security maintenance. A limited amount of that support is in the form of external penetration testing relative to CMS websites including HealthCare.gov.

MITRE is not in charge of security for HealthCare.gov. We were not asked, nor did we perform "end-to-end" security testing. We have no view on the overall "safety" or security status of HealthCare.gov.

MITRE did not and does not recommend approval or disapproval of an Authority to Operate (ATO). Deciding whether and when to grant an ATO is an inherently governmental function which derives from the government's assessment of overall risk posture. In this case, the government made its ATO decisions based on a large set of inputs and factors, among which were the six SCAs performed by MITRE. We do not have visibility into the many other factors that went into the government's ATO decision. CMS did not advise MITRE whether or when ATOs were granted for the Marketplace components tested. In this case, the government made its ATO decisions based on a large set of data.

Again, we were not asked to conduct end-to-end testing. Rather, we tested specific parts of HealthCare.gov within specific parameters established by CMS. We worked alongside the CMS-designated contractor in the course of testing to remediate risks assessed as "high," and in almost all cases we succeeded.

Our testing was accomplished in accordance with standard SCA engineering methodologies. In each case, we assessed component security control risks against CMS-defined security control parameters on a high-moderate-low scale, and we recommended appropriate risk mitigations. On-site Security Control Assessment testing typically begins on a Monday and wraps up within the week. It tests against CMS defined security control parameters. Over the course of the five days of testing, MITRE identifies risks and assigns remediation priorities for risks judged to be at high and moderate levels.

At the committee's request, we previously made available to committee staff the final reports of the six Security Control Assessments relevant to HealthCare.gov. Security testing is designed to flush out and pinpoint the security weaknesses of a digital information system. This enables corrective remediations to be applied and also allows the system operator to make the necessary business judgments and tradeoffs about the overall system.

By definition and design, Security Control Assessment reports will typically contain data that, in the hands of a malicious actor, could be used to compromise the security and privacy of information stored on the affected site. It was, of course, no different in the case of the SCAs performed on HealthCare.gov components. We accordingly redacted from our delivered documents portions that essentially could serve as a technical roadmap to a hacker bent on causing harm.

We also would like the committee to understand and appreciate that, even with the redactions, the information contained in the delivered materials could pose a significant risk to the confidentiality of consumer information accessible through HealthCare.gov.

Because our role in performing the security control tests was limited in both time and scope, MITRE has no insight into how assessed security control risks were handled or what other risks may have surfaced subsequent to the date of testing. Judgments about the potential impact of assessed security control risks on overall system operations or performance were business judgments made by CMS as the operating authority.

Through our broader partnership with the federal government, we remain committed to assisting CMS in working to enhance the care and delivery of health care for all Americans.

I would be happy to respond to your questions. Thank you.