For the Record: Responses to Additional Questions from The Honorable G.K. Butterfield regarding testimony at Energy & Commerce Oversight & Investigations Subcommittee hearing Nov. 19, 2013 of:

Dr. Jason Providakes
Senior Vice President
Center for Connected Government
The MITRE Corporation

1). Can you elaborate on the successes MITRE had in remediating risks assessed as "high" with CMS-designated contractors?

Dr. Providakes:
MITRE has no role in the remediation of risks. MITRE does not remediate findings. We recommend mitigations. It is the responsibility of CMS and its contractors to correct any risks identified during a Security Control Assessment (SCA). MITRE may, at the request of CMS, go back and validate that previously identified risks have been remediated.

Two high risk vulnerabilities were identified as unresolved in the Exchange Consumer Web Services (ECWS) Final Security Control Assessment (SCA) Report dated August 23, 2013. MITRE was not requested by CMS to validate closure of these risks and therefore MITRE has no knowledge of the status of these risks. Those two risks were:

Inconsistent use of security communication protocols: The use of secure computer communications (in the form of encryption standards found in Hyper Text Transport Protocol Secure (HTTPS)) to transport data between the user and the ECWS application was found to be inconsistent, thereby potentially exposing data in transit. MITRE observed that data traffic was sent using an unsecured transport protocol rather than HTTPS encryption.

Several components were not production ready, and MITRE was therefore unable to test some CMS security controls, e.g. Access Control: Several components (e.g., LDAP; Splunk) were not production ready, which meant that MITRE was unable to assess the degree to which certain CMS mandated security controls had been implemented. These limitations were specifically documented in the ECWS SCA Final Report.

2.) Can you discuss some of the security progress that MITRE observed through subsequent SCAs?

Dr. Providakes: MITRE has not been involved in any Healthcare.gov SCAs since the 11 October 11, SCA – "Health Insurance eXchange (HIX) August-September 2013 SCA Report." MITRE is currently conducting an onsite application-only SCA on the Federal Facilitated Marketplace system. The expected completion date is January 9, 2014.

3.) Has CMS outlined a timetable to meet additional outstanding risks identified by MITRE in SCA reports?

Dr. Providakes: MITRE is not aware of any timetable regarding the mitigation of any outstanding risks associated with Healthcare.gov. CMS, in conjunction with its contractors, is responsible for the development and maintenance of the Plan of Action and Milestone (POAM) for remediation of security risks. MITRE has no involvement with POAMs and/or timetables.