FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

October 31, 2013

Mr. Al Grasso
President and CEO
MITRE Corporation
7515 Colshire Drive
McLean, VA 22102-7539

Dear Mr. Grasso:

Pursuant to Rules X and XI of the United States House of Representatives, the Committee on Energy and Commerce is examining the implementation of the Patient Protection and Affordable Care Act (PPACA).

During a hearing before the Committee on October 24, 2013, certain contractors who participated in developing the Federally Facilitated Marketplace (FFM) testified that they did not have adequate time to conduct end-to-end or integrated testing of the FFM website. They also indicated that it was the responsibility of the Centers for Medicare and Medicaid Services (CMS) as systems integrator for the FFM to conduct that testing.

Documents produced during the course of the committee's investigation of problems with the healthcare.gov website show that CMS' failure to conduct adequate end-to-end testing extended to security testing. In a decision memorandum signed by CMS Administrator Marilyn Tavenner on September 27, 2013, Administrator Tavenner acknowledged that the Federal Information Security Management Act (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, 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." A copy of this document is attached.

When Department of Health and Human Services (HHS) Secretary Kathleen Sebelius was questioned about this document at an October 30, 2013, hearing before the Committee, she indicated that the security of the FFM was not compromised because the mitigation plan

referenced in the September 27, 2013, memorandum that was signed by Administrator Tavenner provided for testing and monitoring of the FFM.

We are now seeing the results of HHS' failure to conduct adequate end-to-end performance testing of healthcare.gov prior to its launch on October 1. Almost one month after open enrollment began, the website continues to suffer from glitches and is often unavailable to the public to shop for plans. It is our understanding that your company has contracted with CMS to provide services relating to the security of the FFM. In order to better understand the implementation of the PPACA, including whether the failure to conduct a complete Security Control Assessment increases the risk to the FFM, we ask that you provide the following documents and information no later than November 14, 2013:

1. All Security Control Assessments performed by the Centers for Medicare and Medicaid Services or at the direction of the CMS for the Federally Facilitated Marketplace system and the Data Services Hub.

2. Any and all Authorizations to Operate or Authority to Operate relating to the Federally Facilitated Marketplace system and/or the Data Services Hub.

3. All security mitigation plans or timelines developed by or directed to be performed by CMS regarding the security risks identified by the SCAs.

4. All documents relating or referring to the Security Control Assessments for the FFM, other security testing, the results of any security testing, the schedule for testing, and/or the waiver of any requirements related to the SCA or security testing.

5. Your contract with CMS related to the FFM and all documents relating to work plans, schedules, testing schedules, test results, timelines, status reports, and reviews of your work relating to the FFM. These documents should include, but not be limited to, the Risk Management Plan and all documents, including products or deliverables, referring or relating to risk management; documents referring or relating to industry best practices, recommended standards, and key performance indicators for configuration and operations; the Pre-Operational Readiness Review; and the Operational Readiness Review, including Test Plan and Test Case Specifications, Contingency/Recovery Plan, Implementations Plan, User Manuals, Operation and Maintenance Manual, Training Plan and Materials, System Security Plan, Information Security Risk Assessment, Integration Testing Results, End-to-End Testing Results, Test Summary Report, Defect Reports, Security Testing Results, briefings/presentations to Office of Information Services, Level of Effort estimate to achieve Operational Readiness Review, Project Completion Report, Service Level Agreements, Privacy Impact Assessment, Plan of Action and Milestones (POA + M), Authority to Operate, and Level of Effort estimate to support Operations and Maintenance.

Instructions for responding to the Committee's document request are included as an attachment to this letter. Thank you for your prompt attention to this matter. If you have

questions or wish to discuss your responses or production, please contact Karen Christian or Carl Anderson with Committee Staff at (202) 225-2927.

Sincerely,

Fred Upton
Chairman

Joe Barton
Chairman Emeritus

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

Joseph R. Pitts
Chairman
Subcommittee on Health

Marsha Blackburn
Vice Chairman

Michael C. Burgess, M.D.
Vice Chairman
Subcommittee on Oversight and Investigations

Mike Rogers
Member

Bill Johnson
Member

cc: The Honorable Henry Waxman, Ranking Member

The Honorable Diana DeGette, Ranking Member
Subcommittee on Oversight and Investigations

The Honorable Frank Pallone, Jr., Ranking Member
Subcommittee on Health