1001 Pennsylvania Avenue, NW, Washington, DC 20004-2595 ▪ p 202 624-2500 ▪ f 202 628-5116

crowell moring

Michael Gill
(202) 508-8843
mgill@crowell.com

December 23, 2013

The Honorable Tim Murphy
Chairman
House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
2125 Rayburn House Office Building
Washington, D.C. 20515-6115

Re: Response to Questions for the Record from Creative Computing Solutions, Inc.

Dear Mr. Chairman:

On behalf of our client, Creative Computing Solutions, Inc. ("CCSi"), we are pleased to provide the attached responses to the Subcommittee's Questions for the Record letter.

Sincerely,

Michael Gill
Counsel for CCSi

cc: The Honorable Diana DeGette, Ranking Minority Member

Attachment 1 — Additional Questions for the Record

The Honorable G.K. Butterfield

It is clear that CMS has a robust framework to respond to malicious activity that CCSi adheres to.

a. **Ms. Bauer, does CCSi use both automated and manual approaches to search for malicious behavior?**

Answer: Yes.

b. **Can you provide an example of an anomaly that might prompt CCSi to respond?**

Answer: A foreign (non U.S.) IP address attempting to connect to healthcare.gov.

c. **Would CCSi implement the CMS approved Incident Response Plan (IRP) if any anomaly related to sensitive information was detected?**

Answer: Yes.

d. **At what point might law enforcement be involved under the IRP?**

Answer: CMS would make any decisions to involve law enforcement.

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 Tim Murphy

a. **During the hearing, we asked Mr. Amsler if he had all of the tools and capabilities to successfully and fully monitor the system, he said that "there are some things that we have asked for that are not in place as of yet." You said you agreed with his statement. Please elaborate on why you agree with that statement and how it applies to CCSi.**

Answer: Today's cyber security environment involves constantly evolving threats and equally evolving tools, technologies and techniques to address them. CCSi's objective is to recommend and implement the most robust security approaches for our clients. Those recommendations will evolve and change over time to reflect the current threat environment. Over the course of its contracts, CCSi normally requests additional capabilities to service the client and address the current threat environment. To this end, CCSi along with its subcontractor, compiled a list of additional, potential security measures for CMS to consider.