DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop B3-30-03
Baltimore, Maryland 21244-1850

December 6, 2013

Creative Computing Solutions, Inc.
ATTN: Ms. Maggie Bauer, Senior Vice President of Health Services
1901 Research Blvd., Suite 600
Rockville MD 20850

Dear: Ms. Bauer

Re: Third Party Requests Concerning Security Testing and Evaluation Information

I am writing to provide some guidelines to you about appropriately handling sensitive security testing and evaluation information in response to a request from Congress, or any other third party. As we have conveyed directly to Members of Congress, the Department of Health and Human Services understands Congress' oversight interests in the development of the Healthcare.gov website, and is working to accommodate Congressional requests regarding the website. We understand the importance of working with Congress to respond to requests for information.

At the same time, a top priority for the Department is the privacy and security of consumers' personal information, and the protection of vital IT assets. As you know, the Centers for Medicare & Medicaid Services (CMS) treats this sensitive information as highly confidential because of the serious security risks to the agency's information systems and to the privacy of consumers. Some of the information that you may have collected or produced pursuant to your contract with CMS, if further disclosed, could imperil the security of personal and private consumer information on the Healthcare.gov website and/or undermine the security posture of the Data Services Hub, the routing tool that validates applicant information from various trusted databases through secure networks for purposes of determining eligibility for certain benefits. If handled improperly, this information could provide a roadmap to actors with malicious intent.

Additionally, as you are aware, under your contract, namely **CMS Clause-11 CMS Information Security (APR 2008),** you are required to protect all information and information systems from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction, whether accidental or intentional, in order to maintain the security, confidentiality, integrity, and availability of such information covered by this provision. This provision reads in pertinent part:

> **CMS CLAUSE-11 CMS INFORMATION SECURITY (APR 2008)**
> This clause applies to all organizations which possess or use Federal information, or which operate, use or have access to Federal information systems (whether automated or manual), on behalf of CMS.

The central tenet of the CMS Information Security (IS) Program is that all CMS information and information systems shall be protected from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft—whether accidental or intentional. The security safeguards to provide this protection shall be risk-based and business-driven with implementation achieved through a multi-layered security structure. All information access shall be limited based on a least-privilege approach and a need-to-know basis, i.e., authorized user access is only to information necessary in the performance of required tasks. Most of CMS' information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries, and as such, has access restrictions as required under legislative and regulatory mandates.

The CMS IS Program has a two-fold purpose:

(1) To enable CMS' business processes to function in an environment with commensurate security protections, and

(2) To meet the security requirements of federal laws, regulations, and directives.

Pursuant to the above provision and in order to protect federal information and information systems, you are not authorized to disclose to third parties information collected or maintained by or on behalf of a federal agency, including information collected, or information produced during security testing. The information covered by this requirement includes, but is not limited to, the following information: vulnerability discovered list, ACA Issues list, CMS Monthly Technical Progress Report, POAM reports, Weekly HROB Reports, daily tracker, technical reports, security or network diagrams or drawings, and security event or incident reports.

Given our shared interests in protecting the security and privacy of consumers and of important government IT assets and given that the documents that you may be requested to provide were created pursuant to your contract with us, to protect security we are instituting specific measures consistent with the CMS information security provision in your contract. As it relates to your contract with CMS, you are required to inform me, as Director of the Office of Acquisition and Grants Management, of any requests for ST&E information that you receive from any party, and you may not release documents without authorization from CMS. If you receive a request for this information from Congress, CMS will respond directly to the requestor and will work with the requestor to address its interests in this information.

Sincerely,

Daniel Kane
Director, Office of Acquisition and Grants Management
Centers for Medicare and Medicaid Services