Written Testimony of:

Maggie Bauer
Senior Vice President
Creative Computing Solutions, Inc. (CCSi)

Prepared for:

The House Committee on Energy and Commerce

November 19, 2013

Good morning Chairman Upton, Ranking Member Waxman and distinguished members of the Committee. My name is Maggie Bauer and I am a Senior Vice President at Creative Computing Solutions, Inc. (CCSi). I have responsibility for CCSi's federal health contracts, including: Centers for Medicare and Medicaid Services (CMS); Veterans Affairs (VA); the Department of Health and Human Services (HHS) National Institutes of Health (NIH) and the Military Health Service (MHS). In addition to health-related services, we deliver program and project management services, cyber security services, and enterprise systems engineering exclusively to the federal government. CCSi was founded in 1992 by Dr. Manju Bewtra.

In August of 2012, CMS awarded CCSi a contract to provide security oversight of the CMS eCloud. The eCloud refers to CMS's virtual data center which hosts systems and applications that support the Affordable Care Act. CCSi was competitively awarded this contract in August 2012 under the Alliant Small Business (SB) Government-wide Acquisition Contract (Alliant SB GWAC) which is a Multiple Award, Indefinite Delivery, Indefinite Quantity (IDIQ) contract vehicle. Foreground Security Services (FGS) is our subcontractor on this contract. Together, we are an integrated team of 22 staff members, 6 of whom are CCSi employees and 16 of whom work for FGS.

CCSi's role on this contract is to provide security operations monitoring and management including 24x7x365 security monitoring from a Security Operations Center (SOC). We monitor the perimeter firewalls and network devices for the eCloud and we scan applications for vulnerabilities. These scans do not measure or track availability, up/down times or latency. If we detect an anomaly, we follow the CMS approved Incident Response Plan (IRP) procedures for identified network security configuration flaws and vulnerabilities in network and security devices and in applications. CCSi's contract does not extend to remediating any security configuration flaws or vulnerabilities in the network infrastructure nor does it include remediation of any vulnerability discovered in applications.

CCSi's scope of work also includes configuration, tuning, monitoring and management of CMS government furnished equipment (GFE) that resides in the Terremark security monitoring zone. We review log files, conduct event analysis, and provide reporting on security incidents under the direction and supervision of CMS.

Examples of the functions that CCSi performs under this contract include:

- Detecting malicious activity, preventing unauthorized access to systems, and recommending threat protections

- Maintaining, patching operating and tuning CMS security appliances, tools and services to prevent and detect intrusions
- Ensuring that systems are configured for routine scans and import scan results into security monitoring tools to assess system risk
- Maintaining baseline configuration of the information system and monitor for unexpected changes to the baseline
- Planning and supporting integration of security components of existing tools

Activities involving the development, scaling, testing, release or administration of the Federal Exchange Program System, “healthcare.gov,” the “Federal Exchange” or the Federally Facilitated Marketplace or “FFM” are not within scope of our contract.

I would be pleased to answer any questions that you have. Thank you.