

**Testimony of David Amsler
President and Chief Information Officer
Foreground Security, Inc.**

**Hearing before the House Energy & Commerce Committee
Subcommittee on Oversight and Investigations
“Security of HealthCare.gov”
*November 19, 2013***

Chairman Murphy, Ranking Member DeGette, members of the Subcommittee, good afternoon and thank you for inviting me to testify at this hearing on the security of the web site, HealthCare.gov. I am the President and Chief Information Officer of Foreground Security, Inc. I also founded the company, which provides cyber-security consulting, training and services for both private sector and government entities. Our clients include Fortune 100 companies, smaller but highly-targeted firms, and government agencies. We defend our customers against increasingly intricate threats and threat actors through an integrated approach that entails building security architecture and assessing, monitoring, and responding to attacks against our customer environments.

Foreground Security is a small but growing, dedicated cyber-security business located in Herndon, Virginia and Florida. Our roughly 100 employees are highly-trained and committed to serving our clients.

Foreground Security is one of the companies hired to help develop a robust operational security management program for the new virtual data center created to implement the Affordable Care Act. We are a subcontractor to our teammate, Creative Computing Solutions, Inc.—or “CCSI”—which is the prime contractor for the Centers for Medicare and Medicaid Services (“CMS”).

Our role with CCSI includes a number of objectives relating to the security environment of HealthCare.gov. I think of our role as encompassing three phases. First, is the creation of the security monitoring environment. This entailed getting key staff in place, identifying needed security monitoring software and hardware, and building out a dedicated securities operations center, or “SOC”, from which all monitoring is performed.

Second, is building those security monitoring capabilities identified in phase one into the cloud environment itself. This has been the most challenging part of our contract, in large part because we have had to construct security monitoring capabilities while the system itself is being built. Our work on this phase continues.

And third, is actually monitoring the environment, which itself can be thought of as having two components. One is day-to-day, continuous searching for malicious activities, including reporting and defending against them when they occur. The other is monitoring known, malicious actors or groups in advance of

attacks to proactively identify techniques or tactics they may be using or planning to use to compromise this environment. These are our main, end-state responsibilities relating to the security environment.

We have worked very closely with CMS and Verizon/Terremark on all phases of our work. CMS reviews and approves any capability we place in the environment and Verizon/Terremark, as the host of the environment, helps determine what security measures are placed in the virtual data center.

Perspective on our role is important. While our work for CMS is essential, it is also narrowly focused, and we were not involved in the design of the site, developing the software that runs it, or its administration. To that end, we do not monitor the site for performance purposes. Foreground Security is just one member of the security team. In addition to the other companies represented today on this panel, Verizon/Terremark, URS, CGI, and QSSI all play key roles in developing and testing the security of HealthCare.gov.

I am proud of the work that Foreground Security has undertaken—and continues to undertake—in order to allow families and individuals looking for health insurance to use the HealthCare.gov site, secure in the knowledge that their personal information is being protected with state-of-the art monitoring and defenses. To this point, Foreground Security has fulfilled its obligations to CMS

on time and under budget. We are dedicated to the secure operation of HealthCare.gov and take extremely seriously our obligations to the public trust.

I welcome any questions you may have.