David Amsler
President and CIO
Security and Healthcare.gov

Attachment 1- Additional Questions for the Record

The Honorable G.K. Butterfield

1. It is encouraging to know that numerous highly trained security personnel are continuously monitoring the new virtual data center created for the ACA
    a. Mr. Amsler, does Foreground Security use both automated and manual approaches to search for malicious behavior?

Foreground Security uses a variety of tools to examine network, server, and application activity for matches to known malicious behavior and/or deviations from "normal" user behavior. Through these pattern matching and anomaly detection functions, these tools provide an automated mechanism for identifying malicious behaviors.

Our human analysts review the logs and alerts generated by these tools to differentiate between normal activity that may have triggered an alert and truly malicious behavior. The team also analyzes raw data generated by the healthcare.gov systems and networks to identify malicious behavior the tools may not be capable of detecting. This is a key function, as sophisticated attackers will often change their tactics to avoid automated detection.

    b. If malicious activity is detected, what responsibilities does Foreground Security have to report that activity and who do you report it to?

If malicious activity is detected, our procedures dictate that we gather all relevant details including systems affected, functions and data within those systems that may have been exposed, the nature of the activity in question, users and external systems involved, timeline of events, and other information that helps determine the scope of the incident.

Our team then opens an internal CMS incident case, populates it with those key details, and escalates to the Federal IT Security Manager on duty. Depending on the criticality of the incident, that escalation occurs in as little as 30 minutes and may also include the Director for Marketplace Security, the CMS Chief Information Security Officer (CISO), and other CMS and HHS executive leadership.

c. At what point might law enforcement become involved after malicious activity has been noticed?

Our incident reporting chain includes the HHS Office of the Inspector General (OIG), which provides criminal investigative functions and acts as an interface to other Law Enforcement agencies in cases where an incident is determined to include unlawful activities. That determination is made by the OIG in conjunction with the FBI and other Law Enforcement agencies with whom the OIG liaises.

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

During the hearing, when asked if you have all of the tools and capabilities to successfully and fully monitor the system you said that "there are some things that we have asked for that are not in place as of yet." Please elaborate on what you meant when you said that.

1. Foreground and our partner CCSi maintain a complete list of current capabilities, required tools/capabilities that aren't in place or functioning, and future roadmap items that are requested. That report is provided to the government (COTR and COR) on a monthly basis and I believe examples of that report were turned over to the committee during our extensive document collection effort that included every email, report, or all other documents related to this contract.