12-F-1109 Document 1

HR0011-12-F-0005
Attachment No. 1

Statement Of Work

June 28, 2012

Large Data for Nexus 7, Guard Dog, Adams, and XData Analytics

The purpose of this program is to measure the ability of cloud-based computing infrastructure to support heterogeneous analysis algorithms over multiple large data sets.

Objectives:

Developing a Proof of Concept for global-scale "analytics-as-a-service" with the following attributes:

- High scalability
- High bandwidth throughput
- High quantity of monitored nodes
- Integrating cloud technologies and service delivery models
- Processing of multi-format data sources
- Application design to support cloud enabled data fusion and analytics
- Leverage Contractor's experience in threat actor group composites

Contractor requirements are:

1. Contractor will provide experimental, geographically distributed compute and storage clusters. Contractor performance sites are Miami, FL and/or Culpepper, VA. Contractor will support connectivity to government sites, including DARPA.

2. Contractor, with government assistance, will provide a full implementation of multiple cloud computing software stacks.

3. Contractor will support experimental data sets ranging from 100's of Terabytes to potentially Petabytes. Contractor will assist the government in developing statistical analysis of data trends and volumes, to include base-lining flows under varying conditions. Contractor will support quantifying the impact of multiple data types on large-scale, distributed correlation algorithms and visualization techniques.

4. Contractor will assist in the integration and testing of algorithms to support multiple missions and functions. Multiple tests will be conducted.

5. Contractor will support the quantification of economies of scale through centralization and sharing of compute resources versus geographically distributed compute and storage resources.

6. Contractor will measure baseline performance across various tasks, such as: Extract-Transform-Load, indexing, and exact and inexact searches.

7. Contractor will provide access to existing security tools, collectively known as "ClearSky", as a "Proof of Concept" for testing in an R&D environment the capability to scale to high availability/high throughput analytics. Contractor will test the throughput and accuracy in a high transaction and large scale enterprise-type model. The data to be

ingested and documented by the toolset will be coming from: multiple sources; received in multiple formats; and multiple scales both large and small. The environment may also interface with cloud-based model and host-based models to enhance the Proof of Concept.

8. Contractor will develop and provide "best practices" recommendations for enhanced security, based on experiments run during this program as well as the existing corpus of corporate knowledge.

9. Flexibility and adjustments are expected and will be made during the effort to adapt to new applications and throughput; those adjustments will also be monitored and documented. The Proof of Concept will map existing knowledge of threats and is intended to identify and track new threats as a result of the data and tools we are utilizing across the environments.

Deliverables:

To provide transparent actionable information, metrics, and operational status as follows:

1. Data input into the government provided cloud platform for processing
2. Analytical results for threat, exploit and malware analysis findings and detection observables
3. Threat-actor group tracking and trends with attribution context (when applicable)
4. Bi-Monthly meetings with the government to review operational metrics, discuss data findings, trends and overall project status
5. Internal Program Reviews with government on a monthly basis, and Executive-level Program reviews with the government on a quarterly basis
6. Monthly Status Report/Monthly technical status updates.