Memorandum

**To: Diane Hooie - DOE**

**From: Robert Larmouth – NRECA (Project Manager)**

**CC: Craig Miller – NRECA (Principal Investigator)**

**Carol Hawk, DOE**

**Subject: Update for DOE Project DE-OE0000684: “Energy Sector Security through a System for Intelligent Learning Network Configuration Management and Monitoring”**

**Date: April 4, 2014**

The purpose of this memorandum is to provide an update, highlighting significant accomplishments of the subject project. This is intentionally brief; a more comprehensive account is forthcoming later this month in the form of the quarterly “Research Performance Progress Report”. The team met in Virginia during March and documented the following progress following the 5-layer abstraction model previously discussed.

The Development Team has completed a prototype which implements basic functionality at each of the 5 abstraction layers. For layer 1, sample MultiSpeak® data is being generated in a virtual network environment and collected using an open-source packet capture library. The captured packet data is currently being stored in a Cassandra database (layer 2), where it is accessible to higher layers. The analysis layer and decision layers (layers 3 and 4) are implemented with a custom Java program which defines several sample rules. The analysis layer queries the database and determines if any received packets have violated any existing rules. If a violation is detected, the current decision is to block the traffic. The “block” command is forwarded to the action layer (layer 5), which utilizes the software defined networking (SDN) controller to implement the action. For layer 5, the team is currently using the open-source Floodlight SDN controller and associated APIs in our virtual simulation network.

The Test Team built and demonstrated a prototype device using commodity hardware and several open source software applications (tcpdump, Bro IDS, Afterglow, and Graphviz). This device will serve three purposes. First, it can be used for automated network discovery and visualization. Second, it will perform full packet capture of machine-to-machine protocols to provide research data to the Machine Learning activity. Lastly, the device will be integrated with The Development Team’s recent work to validate its MultiSpeak® protocol generator. In conjunction with the Liaison Team, two electric cooperatives have agreed to deploy the prototype collection device: Benton Rural Electric Association (Washington) and Rappahannock Electric Cooperative (Virginia).

The data analysis by the Machine Learning Team has focused on identifying which data sources and which attributes of those sources will be collected for initial cross-validation experiments on anomaly detection.  The team has converged on five key attributes: sender, receiver, time-stamp, application, and message type.  There are sample data of various types that have subsets of these variables present.  The generation of a large data set with all these features available for all messages is underway.  That data set will be sufficient for testing whether or not it is possible to identify one application masquerading as another and one sender masquerading as another.

The Commercialization Team has reached out to over 50 companies that have expressed interest in this project. The team worked closely with members of the Security Fabric Alliance and, as a result, co-hosted a symposium at NRECA that was attended by 38 of these companies. The team has identified 4 partners that could provide cost share and the business infrastructure for a commercialized product.

In summary, the project is progressing well and the Team is confident of maintaining its obligations and meeting deliverables.