Thomas Moyer (tom.moyer@uncc.edu, Tel: 704 687 8194)
Meera Sridhar (msridhar@uncc.edu, Tel: 704 687 1844)
Weichao Wang (WeichaoWang@uncc.edu, Tel: 704 687 7987)

Department of Software and Information Systems
University of North Carolina Charlotte
Charlotte, NC

Comments on DoE RFI Ensuring the Continued Security of the United States Critical Electric Infrastructure

Response to questions A. (Development of a Long-Term Strategy) 1 and 3:

The power grid is composed of a myriad of devices working in concert to match supply with demand. Many of these devices rely on control hardware and software that are increasingly being networked in order to facilitate management. Another concern with these devices is the fact that many of these controllers are designed and deployed under the assumption that they will only be used on closed networks where security is a secondary concern. However, as Stuxnet has shown, even closed networks are susceptible to compromise. What is needed are tools and techniques that can continuously monitor the behavior of the control devices and provide a range of options for building a more resilient grid.

In this context, resilience can be defined as the ability for a system to deter an adversary from launching attacks, prevent attacks that the adversary does launch, detect successful attacks, and adapt the system to provide continued mission-critical capabilities. What is needed are technologies that will enable robust and trustworthy monitoring of system behavior that can serve as a means of detecting attacks and guide any adaptation that occurs within the system. Such technologies can serve a number of purposes, including early detection of potential attacks, forensic analysis of successful attacks, root-cause analysis of attacks to determine how the adversary compromised the system, and guidance on techniques to prevent similar attacks in the future.

A vital component vulnerable to attack in the electric grid ecosystem is the *safety-critical operating software*, especially software that is internet-connected. In order to address questions (A1) and (A3) and enable the creation of a resilient electric grid system, it is critical to employ a multi-pronged approach to secure the core safety-critical operating software. Critical efforts should include investment in the following research areas and facilitating technology transfer efforts:

1. *Comprehensive vulnerability assessment and attack surface mapping* in existing software and new software procured by US private sector or foreign entities—-state of the art to achieve these include static and dynamic program analysis, and fuzzing (including black box, white box, gray box and artificial intelligence-guided fuzzing)
2. *High-assurance, resilient software*—-a holistic approach is needed to achieve this, including (i) robust testing, including investing in building attack testbeds, software

testing approaches, and automated exploit generation; (ii) software verification; and (iii) applied methods such as causal analysis for anomaly detection and mitigation.

3. *Securing legacy software* already deployed and regularly used in the system (potentially already compromised)---binary hardening methods for retrofitting security into legacy software can achieve this difficult task.
4. *Thwarting continually evolving threats* by monitoring system behavior and understanding how the data used in critical decision making processes evolves over time and also monitoring for anomalous behavior caused by adversary actions through various means.