LETTER OF NOTIFICATION – 2

ESTABLISHMENT OF ADMINISTRATIVE UNIT

(Center, Division or Institute not offering primary faculty appointments or certificate/degree programs)

1. Institution submitting request: University of Arkansas, Fayetteville

2. Contact person/title: Dr. H. Alan Mantooth, Distinguished Professor

3. Phone number/e-mail address: (479) 575-4838 / mantooth@uark.edu

4. Name of Proposed Administrative Unit: Cybersecurity Center on Secure, Evolvable Energy Delivery Systems (SEEDS)

5. Proposed Location: SEEDS will be headquartered at the Cato Springs Research Center (CSRC) on the University of Arkansas campus. Other center activities will occur at the National Center for Reliable Electric Power Transmission (NCREPT) and in individual professor's labs.

6. Distance of proposed unit from main campus: 0 mi.

7. Reason for proposed action: Recognition of a Department of Energy sanctioned university-based center with all of the rights and privileges therein.

8. Mission and role for proposed unit:

The center's overall vision is that future energy delivery systems are able to survive cyber attacks and incidents while sustaining critical functions. To realize this vision, people in power systems engineering, the computer science of cybersecurity, and the power industry will work closely together to identify and analyze needs (i.e., risks and vulnerabilities), research solutions that address these needs, develop tools for rigorous testing, evaluate the efficacy of the solutions as manifest in the tools, and demonstrate these technologies in an industrial setting for R&D purposes in order to evaluate their value for future broader deployment and commercialization potential.

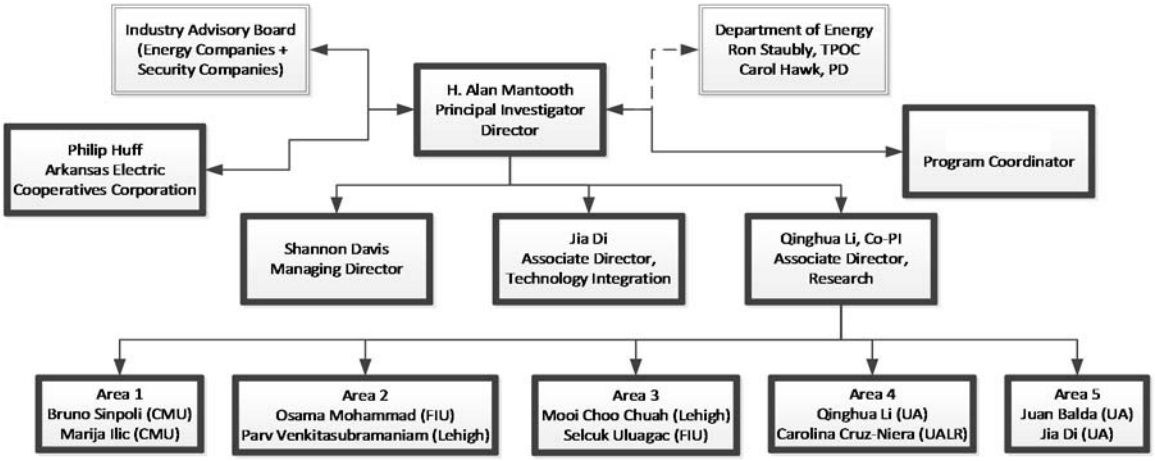
From the cybersecurity perspective, there are three crucial elements for any viable approach to energy systems cybersecurity. First, the proposed technologies and tools should be *integratable* to the current energy control systems without disrupting service, since designing and deploying a new power infrastructure is infeasible. This means that the integration of security technologies should not interfere with the function of the components that they are designed to protect. Second, security technologies and tools proposed for different aspects of energy delivery systems should be easily *composable* to provide more advanced and flexible protections. Since it is impossible to design one solution for all security problems, the natural process is to develop components of security technologies, but the key to success is that these components must be composable to construct systematic solutions. Third, security technologies in energy delivery systems must be *evolvable* to meet future security needs. The energy delivery system is dynamic in nature and cyber attacks evolve with time. Instead of always developing new technologies for new attacks, the cost-effective strategy is that demonstrated R&D technologies can evolve to address new attacks and accommodate new protection needs. In order to meet the goals outlined in this dynamic

approach, the participation of an industry R&D partner is essential. This involvement is critical to address sustainability, as the center must be able to show the national community of utility companies and vendors that tools developed through this center meet these three criteria.

From the power systems engineering perspective, security protection should be provided both to the legacy power grid control and operation functions, which are the core of energy control systems and to emerging power grid components and services such as microgrid and demand-side management as they are integrated into the overall power grid. Protections added to the legacy system should not disrupt a running system or degrade system performance. However, since new components and services are still in their infancy, security features should be built into their design.

This center develops integratable, composable, and evolvable cybersecurity technologies and tools for energy delivery systems to protect both the legacy power grid control and operation systems and emerging components and services.

9. Provide current and proposed organizational chart.



10. Copy of e-mail notification to other institutions in the area of proposed location and their responses; include your reply to the institutional responses.

Not required.

11. Provide additional program information if requested by ADHE staff.

See attachment.

President/Chancellor Approval Date:

Board of Trustees Approval or Notification Date:

Chief Academic Officer: Date: