PRESS RELEASE

From the University of Illinois Information Trust Institute

U.S. Departments of Energy and Homeland Security Establish Major Resilient Smart Grid Program at the University of Illinois

In recent months, the media have been buzzing with talk about the "Smart Grid," especially since then-President-Elect Barack Obama featured the need for new Smart Grid technology in a January 2009 speech on the economy. Now, the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign and its partner institutions have been recruited to contribute towards the ongoing development of a resilient, secure Smart Grid in the United States, following the announcement of a major award of research support from the U.S. Department of Energy with contributions from the U.S. Department of Homeland Security.

The award of nearly $18.8 million over a five-year period to Illinois, Dartmouth College, the University of California at Davis, and Washington State University will fund an ambitious new research program called Trustworthy Cyber Infrastructure for the Power Grid (TCIPG). It reflects a strong consensus that cyber security and resilience will be critical to the realization of a modernized, reliable, and efficient power grid, so that it will be able to guarantee delivery of electricity to consumers and maintain critical operations, even when malicious cyber attacks occur. "Research and development of cyber security tools and technologies for critical controls systems, such as the power grid, are among our top priorities," said Dr. Douglas Maughan, program manager within the Command, Control, and Interoperability Division of the Department of Homeland Security's Science and Technology Directorate. "We're excited to continue working with the Department of Energy and the University of Illinois and its partners in this area of critical need for our nation's security."

Illinois Governor Pat Quinn praised the new program. "The federal investment of over $18 million for a new research program at the University of Illinois underscores our state's critical role as a major contributor to the national process of power grid modernization. I congratulate the U of I team and their partners on this award," Governor Quinn said. "As a result of this program, Illinois homes and businesses will ultimately be able to take advantage of secure technology that will allow them to consume less energy, make greater use of renewable energy sources, and improve the environment."

"I am delighted to share in this announcement," added U.S. Rep. Timothy V. Johnson (R-IL). "The work being done right here at the University of Illinois is critical to the security and reliability of our power grids. As communications systems continue to advance at lightning speeds, the more sophisticated society needs to become to thwart the challenges from those who would do us harm. These scientists and engineers are revolutionizing these security systems and they deserve all the tools we can provide to allow them to do their jobs."

The term "Smart Grid" refers to the integration of the existing physical infrastructure of the power grid with an advanced communication and control cyber infrastructure, with the ultimate goal of making energy transmission and distribution more efficient--- and therefore cheaper for consumers and less wasteful of resources.

However, Smart Grid technologies may themselves introduce new problems, such as increasing the

vulnerability to cyber attack as power grid resources become increasingly linked to the Internet. For example, experts recently warned that some types of "smart" automated meters could be hacked by attackers with minimal equipment and knowledge, and that an attacker who succeeded in gaining access might be able to cause blackouts. Those blackouts could have serious economic and human consequences if they are widespread or affect critical systems, such as airports or city traffic light systems.

"Ultimately, the extent to which the Smart Grid vision is achieved is going to depend on how functional and robust the cyber infrastructure is," explained Ilesanmi Adesida, dean of the College of Engineering at Illinois. "Smart Grid technologies should be able to offer us increased protection against accidents and against adversaries who might want to deliberately harm the power grid, who might include well-funded, highly motivated criminal organizations or even nation-states, not just casual hackers. The concern is that the existing technologies can't offer those guarantees, and that we could even open the door to new risks if we carelessly put together new systems that don't have resilience and security guarantees built in from the ground up. That's where the TCIPG work is going to make a big difference."

Industry experts and regulatory bodies seem to be unanimous in saying that resilience and cyber security are critical areas of concern for the future power grid. "The interconnectedness of the emerging Smart Grid presents cyber security challenges," explains Dave Whitehead, vice president of research & development for Schweitzer Engineering Laboratories, Inc. of Pullman, Washington, a company that works on power system technologies. "The TCIPG researchers have spent years developing solutions to the challenging cyber security problems that are inherent to such complex systems. The new support from the DoE and DHS is going to give them the opportunity to pursue even more innovations." Dr. Arshad Mansour, a vice president at the Electric Power Research Institute (EPRI), agreed that "cyber security is a key component in the development of a smarter grid. EPRI looks forward to continuing to work with the TCIPG team in this critical area." The TCIPG team's past research has been conducted with the active participation of more than 35 power industry entities, which will continue to be involved in the new project.

The TCIPG research team members have been collaborating on work in this area since 2005 under National Science Foundation funding. Their efforts have been devoted to development of resilient cyber infrastructure that is trustworthy, survivable, and efficient. Accomplishments to date include a range of hardware and software solutions, including a highly efficient technique for protecting message exchanges in existing, already-deployed power systems and a strategy for managing complex security policies in large networks that may have thousands of rules controlling who can access what. TCIPG researchers have also addressed the security weakness of smart meters through development of an "attestation" strategy that can detect modifications to software on the meters, thus helping to block attacks and also thwart customers who try to lower their power bills by tampering with their meters.

The new TCIPG research program will involve the development and integration of information technologies with the key properties of real-time availability, integrity, authentication, and confidentiality. More specifically, the objectives are to develop and evaluate technologies needed for realizing select Smart Grid applications, such as wide-area monitoring and control, demand response with controllable load, and plug-in hybrid electric vehicles. Ultimately, the project is expected to result in a secure and real-time communication system, an automated attack response system, and risk assessment and security validation techniques.

William H. Sanders will serve as the Director of TCIPG, with Himanshu Khurana as the Principal Scientist and Pete Sauer as Industry Liaison. Sanders and Sauer are professors in the Electrical and Computer Engineering Department at Illinois, and Khurana is a principal research scientist in the Information Trust Institute. The rest of the TCIPG team consists of professors, research scientists, and students from the four participating universities.

About the Information Trust Institute (ITI)

The Information Trust Institute is a multidisciplinary cross-campus research unit housed in the College of Engineering at the University of Illinois at Urbana-Champaign. It is an international leader combining research and education with industrial outreach in trustworthy and secure information systems. ITI brings together over 90 faculty, many senior and graduate student researchers, and industry partners to conduct foundational and applied research to enable the creation of critical applications and cyber infrastructures. In doing so, ITI is creating computer systems, software, and networks that society can depend on to be trustworthy, that is, secure, dependable (reliable and available), correct, safe, private, and survivable. Instead of concentrating on narrow and focused technical solutions, ITI aims to create a new paradigm for designing trustworthy systems from the ground up and validating systems that are intended to be trustworthy. www.iti.illinois.edu

Contacts: William H. Sanders, 217/390-1311, whs@illinois.edu; Himanshu Khurana, 217/493-8034, hkhurana@illinois.edu

Writer: Jenny Applequist, Information Trust Institute, 217/244-8920, applequi@iti.illinois.edu.

Released October 26, 2009

University of Illinois at Urbana-Champaign