Cyber Security Project Selections

September 23, 2010

These projects have been selected for negotiation of awards; final award amounts may vary.

Lead Research Organization (Partner Organizations)	**Amount**	**Lead Organization Location** (City, State)	***Technology Focus – Application: Project Title*** **Project Description**
1) Innovative Cybersecurity Solutions			
Grid Protection Alliance *(University of Illinois, Pacific Northwest National Laboratory, PJM Interconnection, AREVA T&D)*	$3,215,000	Chattanooga, TN	*SIEGate: Secure Information Exchange for Electric Grid Operations* The Grid Protection Alliance will research, develop, and commercialize a Secure Information Exchange Gateway (SIEGate) that provides secure communication of data between control centers.
Honeywell International *(University of Illinois, Idaho National Laboratory)*	$2,203,653	Golden Valley, MN	*Role-Based Access Control (RBAC)-Driven Least Privilege Architecture for Control Systems* Building upon previous DOE research, Honeywell will research, develop, and commercialize an architecture for critical systems that limits each operator's access and control privileges to the appropriate level for their job function.
Schweitzer Engineering Laboratories *(CenterPoint Energy Houston Electric, Pacific Northwest National Laboratory)*	$2,974,697	Pullman, WA	*Watchdog Project* Schweitzer will research, develop, and commercialize a device for the control system local area network (LAN) that allows only trusted data sources and trusted communication patterns.
Schweitzer Engineering Laboratories *(Dominion Virginia Power, Sandia National Laboratories)*	$1,631,026	Pullman, WA	*Whitelist Anti-Virus for Control Systems Project* Schweitzer will research, develop, and commercialize an anti-virus solution for control systems that prevents the execution of unauthorized code and maintains secure settings and configurations, to be integrated with Schweitzer Engineering Laboratories' substation-hardened computers and communication processor.
Schweitzer Engineering Laboratories *(Tennessee Valley Authority, Sandia National Laboratories)*	$1,117,003	Pullman, WA	*Padlock Project* Schweitzer will research, develop, and commercialize a low-power, small-size plug-in device, referred to as a "dongle," that provides strong authentication, logging, alarming, and secure communications for intelligent electronic devices (IED) in the field. The dongle will detect physical tampering and inform the device developed in the Watchdog Project so that

Lead Research Organization (Partner Organizations)	**Amount**	**Lead Organization Location** (City, State)	***Technology Focus – Application: Project Title*** **Project Description**
			communications received from physically compromised IED are prevented from reaching the control system LAN.
Siemens Energy Automation *(Sacramento Municipal Utilities District, Pacific Northwest National Laboratory)*	$3,153,293	Minnetonka, MN	*Development and Demonstration of a Security Core Component* Siemens will develop and demonstrate a near-real-time cyber and physical security situational awareness capability for the control system environment. It will provide the control center operator with a toolset and training capability to act aggressively as the front line defense against a cyber attack.
Sypris Electronics *(Purdue University Center for Education and Research in Information Assurance and Security, Oak Ridge National Laboratory, Electric Power Research Institute)*	$3,141,187	Tampa, FL	*Centralized Cryptographic Key Management* Sypris will research, develop, and commercialize a cost-effective capability to manage the numerous cryptographic keys assigned to smart meters and other remote devices to secure communications. It will be scalable to accommodate the millions of smart meters within the smart grid advanced metering infrastructure.
Telcordia Technologies *(University of Illinois, Electric Power Research Institute, DTE Energy)*	$3,019,158	Piscataway, NJ	*Tools and Methods for Hardening Communication Security of Energy Delivery Systems* Telcordia will research vulnerabilities in energy sector communication protocols and develop mitigation approaches that harden these protocols against cyber attack while enforcing proper communications within energy delivery systems.
2) National Electric Sector Cybersecurity Organization			
Energy Sector Security Consortium, Inc. (EnergySec)	$5,898,288	Clackamas, OR	EnergySec will strengthen electric sector cybersecurity by establishing a broad–based collaborative public-private partnership; develop cybersecurity solutions to enhance electric infrastructure reliability; provide a path for rapid response to national cybersecurity priorities; supply data analysis and forensics capabilities for cyber-related threat and event assessments; assist in creating a framework to identify and prepare for challenges to grid reliability; share information, best practices, resources, and solutions to and from domestic and international electric sector participants; and encourage key electric sector supplier and vendor support and interaction. EnergySec will form the organization to be known as NESCO.

Lead Research Organization (Partner Organizations)	**Amount**	**Lead Organization Location** (City, State)	***Technology Focus – Application: Project Title*** **Project Description**
Electric Power Research Institute, Inc. (EPRI)	$4,100,000	Knoxville, TN	EPRI will conduct assessment and analysis of cybersecurity requirements and results from groups such as the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corp. (NERC). EPRI will assess existing power system and cybersecurity standards to meet power system security requirements and test security technologies in labs and pilot projects. This project, known as the National Electric Sector Cyber Security Organization Resource (NESCOR), will work collaboratively with NESCO.
TOTAL FUNDING	**$ 30,453,305**		