

Research & Development Subgroup

GCC: Dr. Douglas Maughan, DHS S&T, Program Manager

&

SCC: David Norton, Entergy, Policy Consultant – CIP

ICSJWG 2010 Fall Conference

Meeting Objectives

Review activities from 2010

Discussion and prioritized decisions about 2011-2012 Industrial Control Systems (ICS) R&D requirements

- **Presentations, white board sessions, etc.**

Discussion and decisions about the way ahead

- **Process for publishing WG results**
- **Frequency of “working group” meetings**

Background

- Research and Development Subgroup Chartered in 2009
- Goal:
 - Facilitate communication between industrial control systems stakeholders and the research and development community to ensure effective focus for research and development initiatives and associated funding.
- Milestones:
 - Document current and planned projects with associated details, timelines, and stakeholder involved.
 - Document results of an ICS research and development needs assessment.
 - Prepare a requirements document for sharing sensitive R&D information including an ultimate recommendation as to whether or not a new tool is needed.

Recent Solicitations

DOE FOA:

- **Topic Area 1 – Response to Cyber Attack in Progress**
- **Topic Area 2 – Centralized Cryptographic Key Management**
- **Topic Area 3 – Situational Awareness Data Collection, Analyses, and Visualization**
- **Topic Area 4 – Hardened Platforms and Systems**
- **Topic Area 5 – Secure Communications**
- **Topic Area 6 – Remote Access**
- **Topic Area 7 – Secure Smart Grid Communication Architecture**

DOE Solicitation Awards

<http://www.energy.gov/news/9539.htm>

- **Grid Protection Alliance – *SIEGate: Secure Information Exchange for Electric Grid Operations***
- **Honeywell International – *Role-Based Access Control (RBAC)-Driven Least Privilege Architecture for Control Systems***
- **Schweitzer Engineering Laboratories – *Watchdog Project***
- **Schweitzer Engineering Laboratories – *Whitelist Anti-Virus for Control Systems Project***

DOE Solicitation Awards (cont.)

- **Schweitzer Engineering Laboratories – *Padlock Project***
- **Siemens Energy Automation – *Development and Demonstration of a Security Core Component***
- **Sypris Electronics – *Centralized Cryptographic Key Management***
- **Telcordia Technologies – *Tools and Methods for Hardening Communication Security of Energy Delivery Systems***

DOE Labs - CEDS Solicitation

Cybersecurity for Energy Delivery Systems (CEDS):

- **Project 1 - Configuration Management to Sustain Hardened Cybersecurity Posture**
- **Project 2 - Management of Access Control**
- **Project 3 - Baseline Normal Communications Pattern of Control System Routine Operation**
- **Project 4 - Enhance Existing, Industry-Accepted Power System Reliability Safeguards**
- **Project 5 - Energy-Sector Component Security and Functional Performance Testing**
- **Project 6 - Innovative and Revolutionary Projects to Enhance Cyber Security in the Energy Sector**

DOE CEDS Awards

- **Idaho National Laboratory – High-Level (4th Gen) Language Microcontroller Implementation**
- **Idaho National Laboratory – Control System Situational Awareness Technology Interoperable Tool Suite**
- **Oak Ridge National Laboratory – Automated Vulnerability Detection for Compiled Smart Grid Software**
- **Oak Ridge National Laboratory – Next Generation Secure, Scalable Communication Network for the Smart Grid**
- **Pacific Northwest National Laboratory – Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector**

Requirements Gathering

R&D Requirements that were identified by the working group:

- **Testing Environments (involvement with DETER)**
- **Integrated Approach to Remote Access**
- **Configuration Device Management (Field IED)**
- **ICCP Firewall**
- **Trusted Computers & Anchors Into Systems**
- **Data Analysis and Integrity of Massive Datasets**
- **Identity Management and Credentials Lifecycle**

Requirements Gathering

R&D Requirements that were identified by the working group:

- **Behavior Analysis for Insider Threats**
- **Education Initiatives**
- **Engagement with Associations and Institutions**
- **Expand Use of ICS IP Suite – “OPSAID”**
- **Lab and R&D Outreach Activities**
- **Interdependencies Within Critical Infrastructure**
- **STDS Coordination**

Way Ahead

- **Subgroup will continue to meet to develop milestone products**
 - Refine R&D Needs/Requirements
 - ID further needs
 - Need to determine frequency of meetings
- **Coordinate ICSJWG R&D activities with other government R&D activities**
- **Will continue outreach to additional sectors**

Contact Information

Dr. Douglas Maughan

U.S. Department of Homeland
S&T, Program Manager
(O) 202-254-6145
Douglas.Maughan@dhs.gov

David Norton

Entergy
Policy Consultant – CIP
(O) 504-576-5469
dnorto1@entergy.com

ICSJWG Program Office

ICSJWG@dhs.gov

ICS R&D Subgroup

QUESTIONS?