



# NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

## Control Systems Security Working Group

August 10, 2005 – St. Louis, MO

### Meeting Minutes

**Final**

This meeting of the Control Systems Security Working Group (CSSWG) that is intended to further the dialog between NERC, utilities, electricity sector (ES) groups, other industry sector groups, vendors, consultants, government entities, control system test facilities, and standards organizations to enhance security was announced by email dated July 11, 2005. The NERC Antitrust Compliance Guidelines were read. For purposes of this meeting and these minutes thereof, the term “Control Systems” is taken to include all types of systems that perform direct control, remote set point control, data acquisition, analysis, protection. These systems include (and are not limited to) SCADA, DCS, BTG, Electronic Relays, PLC.

#### Attendees

Tom Flowers, CenterPoint, Chairman  
Linda Nappier, Ameren, Vice Chairman  
Juan Asenjo, Thales e-Security  
Michael Beehler, Burns & McDonnell Engg  
Brent Brobak, AREVA  
Mark Bruen, KEMA  
Jeff Dagle, PNNL  
Robin Goatey, Ameren  
Dennis Holstein, OPUS Publishing  
Rick Kaun, Matrikon

Hank Kenchington, DOE  
Stanley Klein, Open Secure Energy Cntrl Syst  
Thomas Kropp, EPRI  
Roger Lee, Southern Co  
Jim McGlone, DOE  
David Norton, Entergy  
Edmond Rogers, Ameren  
Paul Skare, Siemens  
Bill Winters, Arizona Public Service  
Lou Leffler, NERC

#### Next CSSWG Meetings

Conference call: to be arranged for mid September 2005  
Conference call and WebEx: Wednesday, November 16, 2005 at 1100 edt  
Meeting: Wednesday, December 07, 2005 in conjunction with the NERC Critical Infrastructure Protection Committee meeting in St. Petersburg, FL

#### Motions

Motion – 1: Moved: Stan Klein, Seconded, Action: Passed, no dissenting votes  
Approve minutes of the May 25, 2005 CSSWG meeting, draft – 1, as modified at the meeting.

A New Jersey Nonprofit Corporation

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL [www.nerc.com](http://www.nerc.com)

Motion – 2: Moved: Dave Norton, Seconded, Action: Passed, no dissenting votes  
Approve the agenda for this meeting.

### **Actions**

1. Set up a CSSWG calendar on the working group's NERC Internet site.
2. CSSWG members should advise Tom Flowers or Jeff Dagle of interest in working in the National SCADA Test Bed area.
3. The CSSWG membership list and listserv will be reviewed and managed.
4. Set up listserv for the information/data encryption team.

### **NERC and CIPC Discussion**

The recently enacted Energy Legislation was discussed. The importance of subject matter expert involvement from asset owners and operators in the ongoing critical infrastructure protection response in NERC's anticipated role was stressed.

The current status of the National Infrastructure Protection Plan (NIPP) and the Energy Sector specific plan was discussed. A next step in the NIPP development is the establishment of goals. The Electricity Sector Coordinating Council is engaged in the evolving NIPP. The Department of Homeland Security provided an update to some Electricity Sector representatives on the Protected Critical Infrastructure Information program; those participating had a positive response.

### **CSSWG Work Plan and Path Forward**

The work plan was reviewed with specific attention to the activities in the future.

Security of information and data should be considered from three aspects. The issues for all aspects include private and accurate information/data from point to point, information/data are not viewable by those not authorized, and information/data not alterable by anyone. SCADA requires the protection of data in the real-time monitoring and control of the electric system; timeliness is essential. Market information must meet the same requirements but the timeliness may be somewhat less rigorous than that for SCADA. Critical information whether passed by an email, an email attachment, or physical media (e.g. a disc) must meet the requirements. The three examples may require different security approaches.

Interdependencies exist between the Communications and Electricity Sectors. Concerns include power assurance to and security of the next generation communications networks. Work is proceeding with the recently established Telecommunications Electric Power Interdependencies Task Force (TEPITF). TEPITF reports to the National Security Telecommunications Advisory Committee, and has both communications and electricity participants.

Hank Kenchington described the work of the Technology Roadmap to Secure Control Systems in the Energy Sector and the recent workshop. Tom Flowers and Linda Nappier serve on the roadmap advisory committee. The efforts are beginning to focus in four areas:

1. Identifying Strategic Risks (threats, vulnerabilities, consequences)
2. Security Tools & Practices (prevention, management, development, mitigation)
3. Legacy Systems (options for hardening existing systems)
4. Control System Architecture (securing systems in the future: component improvements and fundamental design changes).

The draft path forward will be circulated for comment to the workshop participants and will then be available, by October 2005 on a collaborative Internet site. CSSWG will be kept apprised of this work, and expects that the Roadmap will be a significant factor in the work plan for 2006.

The matter of numerous standards or standards like documents in the control systems area was discussed. Coordination among the several organizations that are active would be valuable. There may be consideration to joint ownership of tasks in the Energy Sector among AGA, API, NERC, recognizing both similarities and differences of requirements (e.g. data and control actions timing) This may be considered as a NIPP goal.

### **NERC Working Group Procedures**

Refer to the NERC Organization and Procedures Manual in the NERC Operating Manual

<[ftp://www.nerc.com/pub/sys/all\\_updl/oc/opman/New\\_OP\\_Manual\\_2.pdf](ftp://www.nerc.com/pub/sys/all_updl/oc/opman/New_OP_Manual_2.pdf)>

Procedures contained in the manual include membership, meeting quorum, voting, proxy holding.

It is important that the NERC Regions be represented on the CSSWG. It is imperative that the CSSWG remain productive, and the attendees agreed to proceed with this understanding as part of the work plan.

### **National SCADA Test Bed (NSTB)**

Jeff Dagle is the point of contact between NSTB and CSSWG, and he reported on recent activities. Several control and cyber protection systems will be evaluated on the NSTB. A point was made that the ES efforts in this (evaluation) area should be focused using the limited field of ES subject matter experts. It was suggested that testing should include communications using radio.

The AGA-12 cryptographic standard test schedule is not yet finalized; it will be an approximately six month program. Dennis Holstein indicated that key management remains an open issue.

CSSWG members interested in working in this area should advise Tom Flowers or Jeff Dagle.

### **Common Vulnerabilities of Control Systems**

Jeff Dagle reported on analysis done by the NSTB people to suggest mitigations for the NERC list of "Top 10" vulnerabilities. CSSWG should consider prioritizing the list. An issue is current (perhaps limited) and future use of the Internet. There is increasing use of frame relay, along with reduced availability of analog wire. The use of public networks of any configuration should be considered for security and interdependency evaluation; to what extent do ES entities utilize PSTN in some manner for control or control related activities?

A recommendation was made to tie suggested vulnerability list mitigations to the NERC Cyber Security Standard (now in draft) CIP-002-2 – 009-1.

### **Security Guideline: Information Security – Encryption**

Tom Flowers discussed security mechanics of information and data electronic transfer. This includes email, documents, even passing of a document via a disk or USB drive. The draft security guideline contains considerable detail and is an excellent start; more development is required that could lead to a very informative NERC document. The existing Security Guideline: Protecting Potentially Sensitive Information is referenced. Consideration may be given to referencing the Department of Homeland

Security's Protected Critical Infrastructure Information (PCII) program and other programs. The CSSWG agreed to proceed with development of this topic using the security guideline format, recognizing that this work may later be presented as a reference document. Those participating in the development include: Roger Lee (Chair), Stan Klein, Dave Norton, Paul Skare, Dennis Holstein, Robin Goatey, Tom Flowers, Rich Kaun, Bill Winters. A listserv will be established for this group.

### **Outreach Activities**

Attendees reported on the activities of: Electric Power Research Institute; Institute of Electrical and Electronics Engineers; Instrumentation, Systems, and Automation Society; International Electrotechnical Commission; Process Control Systems Forum; Telecommunications Electric Power Interdependencies Task Force.

Cyber exercises are under development. Cyber Storm is Congressionally mandated and being developed by DHS. National Critical Infrastructure Exercise is being developed by the private sector. Both exercises will involve the Electricity Sector. Collaboration between the exercises is being considered.