



NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

Control Systems Security Working Group

December 7, 2005 – St. Petersburg, Florida

Meeting Minutes

Draft-1

This meeting of the Control Systems Security Working Group (CSSWG) that is intended to further the dialog between NERC, utilities, ES (ES) groups, other industry sector groups, vendors, consultants, government entities, control system test facilities, and standards organizations to enhance security was announced by minutes of the August 10, 2005 CSSWG meeting. 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) supervisory control and data acquisition, digital control systems, boiler turbine generator controls, electronic relays, programmable logic controls.

Attendees

Tom Flowers, CenterPoint, Chairman
Michael Assante, INL
Dave Batz, Alliant
Frances Cleveland, Xanthus
Jay Cribb, Southern
Jeff Dagle, PNNL
Frank Dessuit, NIPSCO
Rick Kaun, Matrikon
Hank Kenchington, DOE
Stanley Klein, Open Secure Energy Cntrl Syst

Tom Kropp, EPRI
Bill Loomis, Strategic Partners
Scott Mix, KEMA
Bob Matthews, Pacific Gas and Electric
Bill McEvoy, Northeast Utilities
Dave Norton, Entergy
Mike Peters, DOD
Edmond Rogers, Ameren
Walt Sikora, Verano
Lou Leffler, NERC

Next CSSWG Meetings and WebEx/Conference Calls

Meetings:

Information Security Task Force: Tuesday, January 17, 2006 (morning); St. Louis, MO
Control Systems Vulnerabilities Task Force: Tuesday, January (afternoon) 17, 2006; St. Louis, MO
Control Systems Security Working Group: Wednesday, January 18, 2006; St. Louis, MO
Control Systems Security Working Group: Wednesday, October 11, 2006; St. Louis, MO

WebEx/Conference Calls:

Control Systems Security Working Group: February 15, 2006
Control Systems Security Working Group and Information Security Task Force: April 19, 2006

A New Jersey Nonprofit Corporation

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Control Systems Security Working Group: May 19, 2006
Control Systems Security Working Group: August 16, 2006
Control Systems Security Working Group: November 8, 2006

Motions

Motion – 1: Moved: Dave Norton, Seconded, Action: Passed, no dissenting votes
Approve minutes of the November 17, 2005 CSSWG webex/conference call meeting, draft – 2.

Motion – 2: Moved: Stan Klein, Seconded, Action: Passed, no dissenting votes
Approve agenda for the December 7, 2005 CSSWG meeting as modified at the meeting.

NERC and Critical Infrastructure Protection Committee Updates

The Electric Reliability Organization (ERO) is being developed pursuant to the 2005 energy legislation. Details of this large effort are available at the NERC Internet site <<http://www.nerc.com>>. NERC is the likely organization to be named by the Federal Energy Regulatory Commission (FERC) as the ERO; the ERO will report to the FERC. The FERC is very interested in security of control systems.

Individuals in the ES have provided comments to the Department of Homeland Security (DHS) on the draft Base National Infrastructure Protection Plan (NIPP). A next draft is expected to be released for a short comment period in January 2006.

Scott Mix provided an update on the Cyber Security Standards CIP-002 through -009. It is expected that the standards prepared for ballot will be posted in mid-January 2006 with initial balloting planned for February 2006.

The DHS exercise Cyber Storm that will examine the communications during a series of cyber events will be conducted during the week beginning February 6, 2006. Several ES entities are participating.

The DHS Process Control Systems Forum (PCSF) <<https://www.pcsforum.org/>> supports several interest groups. One of these is the Crisis Management Interest Group that will explore the recognition of and response to a cyber attack that intrudes control systems with resultant infrastructure impacts. Elements of crisis management likely include: overall situational awareness, means to identify a potential, imminent, or occurring crisis, immediate operational response, recovery, and — during it all — the absolutely requisite communications including inter-sector coordination. Anyone working with the CSSWG is invited to participate; please contact Lou Leffler <lou.leffler@nerc.net>.

The Telecommunications Electric Power Interdependencies Task Force (that reports to the National Security Telecommunication Advisory Committee is actively pursuing the interdependencies with focus on recovery. The dependence of the ES on the communications sector is a matter that requires further definition and likewise the ES's dependence on the Internet.

CSSWG Work Plan

Stuart Brindley, CIPC chairman, addressed the CSSWG and left the strong message that the work of CSSWG is and will continue to be very important to the security of the bulk electric system and “enormously helpful” in implementation of the Cyber Security Standards CIP-002 through -009.

The accomplishments by CIPC are largely led by the working groups and task forces resulting in consensus decisions at all appropriate levels. It is imperative that subject matter expertise is enjoined from asset owners/operators, industry sector groups, vendors, consultants, government entities, control system test facilities, and standards organizations. CSSWG routinely votes on agendas, minutes, and recommendations to CIPC. The voting member list will be established and incorporated within the CSSWG work plan that was approved by CSSWG and is being presented to the CIPC for approval.

Common Vulnerabilities of Control Systems

The mitigations suggested to deal with the common vulnerabilities are developed at three levels: foundational, intermediate, and advanced. The common vulnerabilities list together with mitigations will be updated by the Control Systems Vulnerabilities Task Force, chaired by Robin Goatey, working with the National SCADA Test Bed.

Roadmap to Secure Control Systems in the Energy Sector

Hank Kenchington discussed the status of the roadmap. The steering committee is completing the plan that will be made available for comment. The involved organizations must then take ownership of the roadmap and execute the designated path forward.

National SCADA Test Bed (NSTB)

Jeff Dagle reported as the point of contact between the National Labs involved in the NSTB and the CSSWG. The NSTB is proceeding with testing related to the ES on the AGA-12 standard, Modbus, DNP-3. Performance will be evaluated concerning latency and baud rates. The strength of the encryption algorithm and implementation security, bench test, and field test will be conducted. The overall NSTB test plan is being completed. Active asset owner/operator participation is strongly encouraged.

Cyber Risk Project

Michael Assante presented the subject project that is being developed to determine “ground truth” in the risk scenarios that will be used to better assure a good understanding of the risk associated with cyber security of control systems. The results may be valuable to asset owners/operators and others that have strong interest in assuring the reliability of the bulk electric systems. The initial intent is to focus on control system risk related to a broad spectrum of potential threats; follow-on work may explore the implications for the grids. This work can then lead to better understandings and development of more effective mitigatory actions. This effort will also provide the ability to assess the risk of new announced threats. There should be focus on five plus years into the future within a routed environment.

Security Guideline: Information Security – Encryption

The draft version 0.03 of the subject document was reviewed. The primary audience for this security guideline is the user who needs secure document and email handling. There may be two parts to the document: one to provide basic guidance and one to delve into technologic solutions.

The continuing work on this product will be guided by the Information Security Task Force, chaired by Tom Flowers.

Liaisons

The International Electrotechnical Commission TC 57, WG-15 is developing security measures for the Inter-control Center Communications Protocol.

The Institute of Electrical and Electronics Engineers is developing security for protective relays, intelligent electronic devices, and wireless technologies.

The SANS (SysAdmin, Audit, Network, Security) Institute will conduct a SCADA Summit, 01-03 March 2006. Courses in security will be available on the first day. The object of the summit is to provide “project illumination” and user-developed security solutions.