



# NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

## Control Systems Security Working Group

January 18, 2006 – St. Louis, Missouri

### Meeting Minutes

**Final**

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 December 7, 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. A quorum of CSSWG members was present.

#### Attendees

Tom Flowers, CenterPoint, Chairman  
Linda Nappier, Ameren, Vice Chairman  
Michael Assante, INL  
Andrew Bartels, Aegis Tech  
Brent Brobak, Areva  
Jeff Dagle, PNNL  
Frank Dessuit, NIPSCO  
Robin Goatey, Ameren  
Dennis Holstein, Opus Publishing  
Rick Kaun, Matrikon  
Stanley Klein, OSECS

Scott Mix, KEMA  
Bob Mathews, Pacific Gas and Electric  
Dave Norton, Entergy  
Prudence Parks, UTC  
Edmond Rogers, Ameren  
Robert Sill, Aegis Tech  
Paul Skare, Siemens  
Joe Weiss, KEMA  
Tobias Whitney, Burns and McDonnell  
Lou Leffler, NERC

#### Next CSSWG Meetings and WebEx/Conference Calls

##### Meetings:

Control Systems Security Working Group: Wednesday, October 11, 2006; St. Louis, MO

##### WebEx/Conference Calls:

Control Systems Vulnerabilities Task Force: February 21, 2006

Control Systems Security Working Group: February 28, 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](http://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: Bob Mathews, Seconded, Action: Passed, no dissenting votes  
Approve agenda for the January 18, 2006 CSSWG meeting.

Motion – 2: Moved: Stan Klein, Seconded, Action: Passed, no dissenting votes  
Approve minutes of the December 7, 2005 CSSWG meeting, draft – 1.

## **Common Vulnerabilities of Control Systems**

The Control Systems Vulnerabilities Task Force is developing a 2006 Top Vulnerabilities of Control Systems and Mitigations list that will include mitigations that are foundational, intermediate, or advanced in scope.

## **Information Security**

The Information Security Task Force continues development of guidance that can be used regarding security of email and other electronic documents. A review of the existing security guideline: Protecting Potentially Sensitive Information, together with this effort will be conducted.

## **Zero Day Event Detection / Correlation**

A subject reference document is proposed. Discussion resulted in the following concepts and action plan for a Zero day event; an event happens or is anticipated to happen imminently that impacts or may impact control systems:

1. What would an asset owner/operator do?
  - A. Gather information
  - B. Evaluate actions
  - C. Prioritize
  - D. Mobilize and take action
2. Operator detection of an emerging event that is just starting.
3. A Day One event that has been identified but not corrected.
4. A Zero Day event has no pre-alert and commences, perhaps on “your” system or on another system. So, the Zero Day event for the first entity becomes known and then is a Day One event for others that have not yet been impacted.
5. Question: How does the Zero Day system discover the event?
6. Distinguish between an event caused by malware that had been installed for some prior time period and an event that is caused at the time observed.
7. Response (incidence response) commences once the event is known as a capability or observed in actuality (two separate initiations of actions).
8. Zero Day is triggered on suspicion of or occurrence of an event. Zero Day ends upon certainty that an event has occurred. Zero Day includes incidence response to the point of confirmation that an “attack” has occurred.
9. Day One is triggered when it becomes known that a threat exists.
10. Scope of the reference document is the preparation for, detection of and actions to an event between Zero Day and Day One.
11. Need a “preamble” that clearly lays out the subject of the reference document.

12. Use accepted security definitions (e.g. Zero Day), or leave the terms out of the document.
13. Focus on the means to detect that an event is or has occurred. These “sensors” may be tuned to anticipate an impending event.
14. An event may be of system immediacy or of possible future concern, e.g., immediacy: system operations occurring without logical causation. Future concern: anomalous computer activity, IDS alarm.

Who	What	When
Bob Matthews	Baseline control systems network activity, states, loading, processes	10 Feb
Joe Weiss	Review case histories re: Zero Day, Day One, detection/correlation (sanitized)	10 Feb
Stan Klein Paul Skare	What to do when suspicious, initial response	10 Feb
THE Ameren Team	Write the risk decision and baseline detection parameters. Operations perspective of the event timelines.	10 Feb
Prudence Parks	Liaison with UTC.	10 Feb
Scott Mix	Draft the “preamble”, definitions, terms	10 Feb
Mike Assante	Process: event analysis through to incident identification.	10 Feb
Brent Brobak	Notification to operators of emerging events. Describe vendor response to an urgent RFI.	10 Feb
Tobias Whitney	List of scenarios and relevant data sources for correlation	10 Feb
Tom Flowers Lou Leffler	Receive and collate all responses into workable form	11 Feb

Send responses to Tom Flowers and Lou Leffler by 10 February 2006.

### Incident Response – Cyber and Physical

A subject security guideline is proposed. Discussion resulted in the following concepts and action plan:

1. When do you know (with certainty) that the causation of an event was malicious or not?
  - A. Assume serious incident has resulted in an investigation.
  - B. There may be rare scenarios that do not lead to certainty.
  - C. Need to gather the right information. What is the right info to gather? Past events may guide.
  - D. Multiple occurrences at several locations.
2. How often and under what conditions do you initiate your Incident Response Team (IRT)?
  - A. IRT procedures need not be “onerous”.
  - B. Incident response can lead to improved control systems based upon the investigations and subsequent lessons learned.
  - C. Composition of IRT.
  - D. When initiate the IRT activity.
  - E. What information to be developed by IRT.
  - F. How fast to initiate.
  - G. Initial response expectations.

- H. Question for answer in an “hour”: Is there any evidence whatsoever of anything malicious occurring coincident with the event (whether or not know at this time if related to the event)?
- I. What results in a report, and to whom?

An Incident Response Security Guideline will be supportive of related Standards. Guidelines are not mandatory. A security guideline may be developed so that a large percentage of the electric sector could be reasonably expected to meet them if so desired.

Consider starting with available Incident Response Plans, from those entities that have such plans in place. Realize that existing plans may be subject to some or substantial enhancement. Note taken that many existing plans may not include a substantive cyber component. Consider plans from other sectors, because this may not be especially specific to control systems “vs.” other business systems.

Who	What	When
Tom Flowers Frank Dessuit THE Ameren Team	Present Incident Response Plan	10 February
Tom Flowers Lou Leffler	Receive and collate all responses into workable form	12 Feb

### 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 overall 2006 NSTB test plan is underway. The NSTB is proceeding with testing related to the electric sector on the AGA-12 standard; this testing is expected to be complete by the end of March 2006.

### Liaison

Dennis Holstein presented on key management. The concept will be presented to the Public Key Infrastructure Task Force for consideration.

Stan Klein reported on recent Institute of Electrical and Electronic Engineers (IEEE) activities related to the work of the CSSWG. The Substations Subcommittee is considering a security standard for substation intelligent electronic devices (exclusive of relays). The ISA and IEEE are considering a standard for wireless controls. There is work on configuration control for relays including patch management.

### Other Discussion

The CSSWG Work Plan that has been approved by the Critical Infrastructure Protection Committee with the addition of members and associates was reviewed.

The Security Guidelines Working Group will be asked to advise the CSSWG of those existing security guidelines that the CSSWG should review for consistency and currency.

The status of the proposed Cyber Security Standards CIP-002-1-009-1 was discussed regarding final posting, WebEx, and balloting.