

NERC News

January 2009

HEADLINE NEWS

Network "Hydra"

NERC working to establish a group of industry cyber experts to handle modern fast-moving threats to the bulk power system.

[To read more click here >>](#)

NERC and Regional Entity Self-Assessment

Comments Sought for NERC and Regional Entity Self-Assessments by February 25, 2009.

[To read more click here >>](#)

Reliability Impacts of Climate Change Initiatives (RICCI) Task Force

New task force to set course for future studies of reliability impacts of climate initiatives.

[To read more click here >>](#)

Integrating Variable Generation

Comments on the Integration of Variable Generation Task Force (IVGTF) report are due by Friday, January 30th.

[To read more click here >>](#)

STANDARDS NEWS

Drafting Team Vacancies

NERC has a number of standards drafting teams seeking expertise.

[To read more click here >>](#)

Reliability Standards Under Development

Keep track of and link to proposed reliability standards under development.

[To read more click here >>](#)

COMPLIANCE NEWS

WECC Certified as a Reliability Coordinator

On December 23, 2008 NERC certified Western Electric Coordinating Council (WECC) as a Reliability Coordinator.

[To read more click here >>](#)

NERC Continues to File Notices of Penalty

New notices of penalty are now available.

[To read more click here >>](#)

FILINGS

NERC Filings/FERC Orders

Documents filed with FERC and Canadian authorities over the last month.

[To read more click here >>](#)

FEATURE ARTICLE

Suspicious Probes of Interest for the Electric Sector

Hundreds of thousands to millions of probes are thrown against electric power organizations' outer defenses every day.

[To read more click here >>](#)

HEADLINE NEWS

Network “Hydra”: Connecting Electric Industry Subject Matter Experts for the Greater Good*January 23, 2009*

Modern threats to the bulk power system are swift, relentless, ever-changing and stem from an immeasurable number of offenders. Various threats extend from cyber activity to physical destruction to terroristic intimidation from offenders attempting to uncover vulnerabilities. NERC, operating as the ES-ISAC, is charged with identifying the latest vulnerabilities, determining mitigation plans and educating the industry on ways to secure their physical and cyber assets to avoid potential failure.

Enter Network ‘Hydra’, a program designed to engage the right people with the right process at the right time to dynamically protect the electric sector.

Hydra will create a network of electric industry subject matter experts (SME) to handle modern fast-moving threats to the bulk power system. The program will identify and manage security knowledge resources as part of the ES-ISAC business processes and workflows. Hydra participants will be asked to assist the ES-ISAC to generate the highest quality threat warning and vulnerability management intelligence. Hydra embraces a set of tools and methods that allow SMEs to collaborate effectively in an expert social network.

An Open Invite

Hydra is seeking 200 individuals that are directly employed by bulk power system and electric sector entities with the following backgrounds:

- Cyber security
- Physical security
- Operations
- Infrastructure Support (technology and supply chain)

There is an open invitation to anyone employed by an electric sector entity with an ES-ISAC performed verification. The ES-ISAC’s goal is to complete all verifications in a one week timeframe.

Hydra participants are expected to:

- Commit to adhere with information protection requirements
- Complete a skills and experience questionnaire
- Participate in readiness tests and receive ES-ISAC Hydra notices
- Participate if able (goal of participating in 4 calls a year)
- Actively contribute in calls to analyze/evaluate specific threats or vulnerabilities
- Advise the ES-ISAC as requested (e.g. bulk power system & electric infrastructure impact analysis)

In 2009 the ES-ISAC will attempt to consistently employ Hydra on every formal notification sent to the electric sector. Active Hydra members will routinely evaluate the effectiveness of the program and improve associated processes and methodologies.

NERC will attempt to launch efforts to assemble a Hydra team in late March, 2009. More information will be provided via the NERC web site (<http://www.nerc.com/>) as the registration date approaches. ■■■

Comments Sought for NERC and Regional Entity Self-Assessment*January 14, 2009*

NERC is required to submit an assessment of its performance to the Federal Energy Regulatory Commission three years from the date of certification as the Electric Reliability Organization. The initial performance assessment report is due to the Commission by July 20, 2009. As the first step in developing the performance assessment filing, NERC is seeking input from users, owners, and operators of the bulk-power system, and other interested parties.

To facilitate stakeholders and other interested persons in providing focused input to the performance assessment, NERC and the Regional Entities (REs) have prepared [self assessment documents](#) and an [on-line survey](#). [Click here](#) for the cover sheet that more

HEADLINE NEWS *(continued)*

fully explains the approach to developing the performance assessment filing, and [click here](#) for the instructions for the on-line survey. NERC and the REs encourage each entity to complete the on-line survey and to provide written comments to pa2009@nerc.net. A copy of the survey is available [here](#) for use in developing comments prior to completing the survey on-line.

The deadline for completing the [on-line survey](#) and submitting written comments is **February 25, 2009**. Questions about the performance assessment process should be sent to pa2009@nerc.net. ■■■

Reliability Impacts of Climate Change Initiatives (RICCI) Task Force

January 28, 2009

Federal, state, and provincial CO₂ legislation is pending throughout North America. A special reliability assessment is vital to quickly evaluate a variety of CO₂ legislative scenarios and their impact on bulk power system reliability. For NERC to perform this vital independent assessment in a timely manner, assistance from consultants is required.

The study will go beyond the regional view and 10-year assessment period, and develop a continental/regional assessment, enabling a consistent reliability “measuring stick” evaluating regional and North American concerns.

The PC Chair will appoint a chair and PC members with resource planning and transmission planning expertise for the task force. The task force will have at least one person from each interconnection to ensure that regional/geographical diversity is represented. Industry experts may be appointed as well.

Please contact Mark Lauby at mark.lauby@nerc.net if interested in becoming part of this task force. ■■■

Integrating Variable Generation

January 28, 2009

This Special Report, [Accommodating High Levels of Variable Generation](#), describes the characteristics of variable generation and identifies changes to planning and operations practices techniques and tools required to reliably integrate large amounts of variable generation into the bulk power system.

Comments on the Integration of Variable Generation Task Force (IVGTF) report are due by Friday, January 30th. The report will be presented to the Planning Committee for its approval in March. ■■■

NERC Trivia

What is the name of the cartoon character that acted as corporate spokesman for electricity generation in the United States for some six decades?

(see page 8 for the answer)

STANDARDS NEWS

Reliability Standards Under Development

The [Reliability Standards Under Development](#) web page helps stakeholders keep track of proposed reliability standards under development. The

summary below shows standards out for comment, review, or balloting.

Reliability Standards - Under Development			
Standard Title	Action	Start Date	End Date
Current Ballots			
Project 2008-16 — Transmission Operations Violation Severity Levels (TOP-004-2)	Recirculation Ballot	01/28/09	02/06/09
Project 2006-07 — ATC/TTC/AFC and CBM/TRM Revisions (MOD Standards)	Recirculation Ballot	01/20/09	01/29/09
Posted for 30-day Pre-ballot Review (Open Ballot Pools)			
Project 2008-09 — Regional Entity Compliance Managers Request for Interpretation — EOP-001-0, Requirement 1	Join Ballot Pool	01/28/09	02/26/09
Posted for Comment			
Project 2009-06 — Facility Ratings	Comment Form	01/20/09	03/05/09
Project 2009-07 — Reliability of Protection Systems	Comment Form	01/20/09	02/18/09
Project 2008-14 — Cyber Security Violation Severity Levels Revisions	Comment Form	01/12/09	02/10/09
Project 2006-07 — ATC/TTC/AFC and CBM/TRM Revisions (MOD Standards)	Comment Form	01/07/09	01/28/09



Drafting Team Vacancies

NERC has a number of standards drafting teams seeking expertise. Participation on a drafting team provides stakeholders an excellent opportunity to become familiar with the standards development process, play a pivotal role in improving electric reliability, and interact with industry peers interested in similar issues. For a list of vacancies please visit the following site:

http://www.nerc.com/filez/standards/drafting_team_vacancies.html

One drafting team is currently in the nomination period. The Standards Committee is seeking industry experts to serve on the Reliability of Protection Systems Standards Authorization Request (SAR) Drafting Team. The SAR proposes drafting a standard to require facility owners to have protection systems installed such that the failure of one of the specified components of a protection system would not prevent meeting the Bulk Electric System performance specified in the Transmission Planning (TPL) standards. More information about the project is available on the following page:

http://www.nerc.com/filez/standards/Project2009-07_Reliability_of_Protection_Systems.html

The SAR drafting team will assist the requester in further developing the SAR and considering stakeholder comments. If you are interested in serving on this drafting team, please complete the following electronic nomination form by February 3, 2009:

<https://www.nerc.net/nercsurvey/Survey.aspx?s=48b95d5be23b46bf80f14d58acb2f290>

Any industry stakeholder meeting the indicated qualifications for the vacant appointments can submit a self nomination form to sarcomm@nerc.com. Please contact Dave Taylor at david.taylor@nerc.net or at 609-651-5089 with questions regarding drafting team vacancies. ■■■

WECC Certified as a Reliability Coordinator

On December 23, 2008 NERC certified Western Electric Coordinating Council (WECC) as a Reliability Coordinator (RC) on a conditional basis. The certification process was completed in reasonable accordance with the NERC Rules of Procedure 500 and Appendix 5 to determine if the applicant has the necessary tools, processes, and procedures to perform the function as a NERC certified RC. The applicant presented to the Certification Team the necessary evidence for its review, as it relates to the applicable standards/requirements and good industry practices for sustained reliable RC operation of the western interconnect. Because of this review, the Certification Team has reasonable assurance the WECC RC does have the tools, processes, and procedures in place to reliably perform the RC function.

Five site visits were conducted; three were conducted at WECC's new control center located in Loveland, Colorado on October 8-10, 2008, November 17, 2008, and December 15-18, 2008. Additionally, two others were conducted at WECC's control center in Vancouver, Washington on October 13-17, 2008 and, November 17, 2008.

WECC RC began operation in their new facilities on or about January 1, 2009. ■■■

FILINGS & ORDERS

NERC Filings to FERC

(click on the filing to view)

January 12, 2009

Comments on WECC Regional Reliability Standard Regarding Time Error Correction

Docket No. RM08-12-000

January 7, 2009

Comments on Specific Requirements of Frequency Response and Bias and Voltage and Reactive Control Reliability Standards

Docket No. RM08-16-000

FERC Orders to Note

(click on the order to view)

January 27, 2009

Order on CIP VRFs Compliance Filing

Order approving 12 revised and 9 new VRFs. In addition, the Commission requires revisions to four of the new VRFs.

Docket Nos. RM06-22-002 and RM06-22-003

January 22, 2009

Letter Order approving two revised versions of Reliability Standards

Order approving two revised Reliability Standards (IRO-005-2 and TOP-004-2) NERC filed on July 28, 2008.

Docket No. RD09-1-000

January 16, 2009

Notice of Extension of Time - Constellation Appeal

Extension of time to submit a compliance filing in response to the Commission's Order Remanding Compliance Registry Determination to the ERO issued November 20, 2008.

Docket No. RC08-7-000

January 16, 2009

Letter Order Accepting November 17 Compliance Filing

in response to Order No. 716: Nuclear Plant Interface Coordination Reliability Standard.

Docket No. RM08-3-002

January 16, 2009

Notice of Penalty - Duke Energy Carolinas, LLC

Order stating FERC would not review the Notice of Penalty filed regarding Duke Energy Carolinas, LLC.

Docket No. NP09-3-000

January 15, 2009

Order Granting Clarification – 2009 Budget Order

Clarification of the October 16, 2008 Order on the 2009 Business Plan and Budget.

Docket No. RR08-6-001 and RR07-14-002

January 15, 2009

Guidance Order on Conducting Compliance Audits by the ERO and Regional Entities

Docket No. AD09-3-000

January 15, 2009

Order Approving Audit Report, Determining Issue of Separation of Functions and Directing Actions

Approves the Audit Report on Southwest Power Pool's separation of functions.

Docket No. PA08-2-000

January 15, 2009

Extension of Time - NERC and NPCC Submission of Data Request

Grants NERC's and NPCC's January 14, 2009 joint motion for extension of time to submit a compliance filing in response to the Commission's December 18, 2008 Order Directing the Submission of Data. The extension is granted to and including February 20, 2009.

Docket No. RC09-3-000

January 9, 2009

Order Accepting Notice of Penalty filed on December 12, 2008, stating FERC would not review the notices on its own motion.

Docket Nos. NP09-1-000 and NP09-2-000

FEATURE ARTICLE

Suspicious Probes of Interest for the Electric Sector

Mike Assante, Vice President and Chief Security Officer, NERC

Hundreds of thousands to millions of probes are thrown against electric power organizations' outer defenses every day. This activity is not unique to the electric sector and a majority of the scanning activity can be classified as routine "noise" (or normal opportunistic) that occurs across the Internet. Many of the probes against Internet gateways constitute network scanning. The source of this activity is often a compromised victim computer or an attacker's computer which is sending a connection request to a large list of possible network addresses listening for replies that indicate a targeted computer possess a vulnerability.

To draw an analogy, if the Internet was a neighborhood it could be classified as a high-crime area with a lot of unsavory activity occurring on the streets in plain view. Each of your organization's internet facing networks would be home sitting somewhere on a block in this tough neighborhood. The activity described above, is like having random people walking up and down neighborhood blocks checking windows and doors, hoping to find an unlocked and unguarded opening to let them in. The activity can be referred to as non-directed, meaning they are checking all houses on a block or several blocks to find a weakness to exploit.

Even non-directed activity can be dangerous, as it often serves as a pre-cursor to an attack if a weakness is revealed. There are many threat actors that once they have successfully compromised a network and discover its owner and purpose will look to maximize their gain by using your computer resources, finding valuable data, or by selling access to your network to others.

One can argue that directed probes have a higher likelihood of success or might carry more negative consequences. A directed probe might indicate the attacker is looking for a specific type of weakness (to support their ultimate objective) or be focused on an individual organization's networks and not large pools

of internet connected machines. In the neighborhood analogy a directed probe would either be a would-be attacker that only jiggles door knobs on exterior facing garage doors or is ignoring everyone else's house to only concentrate on homes owned by a specific person. In the physical world this type of activity would ratchet up the homeowners responses to these types of threats.

The ES-ISAC is very interested in tracking probes that are looking for weaknesses associated with specific devices or applications. The ES-ISAC is specifically interested in probes looking for unique or common electric sector operational systems and applications, for example network ports commonly used for SCADA or control systems. (It is important to note that activity targeting control system associated ports may not be specifically targeting control system as many broad range scans will walk through high-ports not necessarily looking for anything specific. Also, the traffic can be legitimate control system traffic or the port can also be associated with other more general networking applications.) Characteristics of observed activity on control system associated ports that might be highly suspect would include short or long duration of the scan, analyzing all the scanning activity coming from the offending source and ruling out broad range scanning, and looking for re-occurrence or spikes.

Here are some examples of high interest network scanning activity by port:

- Port 102 – Potential ICCP Activity
- Port 502 – Potential Modbus TCP Activity
- Port 20000 – Potential DNP3 over IP Activity

Since a network scan or probe can serve as a precursor to an attack it can be very beneficial to characterize this activity and look for suspicious activity. The profile of scanning activity will often be a function of the attacker's source computer, Internet location, choice of scanning tools, or objectives.

Here is a quick summary of methods to profile scanning activity and assist in determining suspicious activity:

FEATURE ARTICLE *(continued from previous page)*

- Analyze and characterize all the activity coming from a source
 - Look for specific interest in select ports (e.g. hotlist all control system related ports)
 - Correlate activity across multiple internet addresses, if applicable
 - Correlated activity on gateways with address separation is a good indicator that the scanning is directed to your organization
- Look for activity over time from specific sources (try to identify re-occurrences separated by time)
- Analyze the specific packet pattern
 - Number of hits per address
 - Number of packets sent (small number can indicate unique technique)
 - Number of probes per time unit (seconds)
 - Time between probes

The ES-ISAC considers suspicious probes as a cyber event vice a cyber incident. A probe that identified a vulnerability that was successfully exploited by a follow-on attack (resulting in a compromise of your outer defenses) would constitute a cyber incident. Cyber incident reporting is required under CIP-008-1, but voluntary cyber event reporting is encouraged when an organization feels the activity is suspicious or unique.

Instructions for Voluntary Reporting: Please send an e-mail to the esisac@nerc.com to voluntarily report a suspicious cyber event. The reporting entity can provide details in the response e-mail or indicate an affirmative finding and specify a preferred method for ES-ISAC staff follow-up. ■■■

Attend the
National Electricity Delivery Forum
February 18-19, 2009
Renaissance Washington Hotel
Washington, DC

The only forum co-sponsored by DOE and NARUC, this conference will address challenges to modernizing the U.S. grid.

Visit: <http://www.electricitydeliveryforum.org/>

Answer to NERC Trivia:

What is the name of the cartoon character that acted as corporate spokesman for electricity generation in the United States for some six decades?

Reddy Kilowatt. Reddy was invented by Ashton B. Collins, Sr., who worked for Alabama Power Company. Reddy debuted on March 11, 1926 as the symbol for electric service.

CAREERS AT NERC

Benchmarking Technical Analyst

Princeton, NJ

Details:

<http://www.nerc.com/files/Technical%20Analyst-Benchmarking.pdf>

Compliance Investigator

Princeton, NJ

Details:

<http://www.nerc.com/files/Compliance%20Investigator.pdf>

Data Management System Specialist

Princeton, NJ

Details:

<http://www.nerc.com/files/DataManagementSystemSpecialist.pdf>

Engineer of Organization Registration

Princeton, NJ

Details:

<http://www.nerc.com/files/Engineer%20of%20organization%20registration.pdf>

Engineer of Reliability Performance and Events Analysis

Princeton, NJ

Details:

<http://www.nerc.com/files/EngineerofReliabilityPerformanceandEventsAnalysis.pdf>

Manager of Critical Infrastructure Protection

Princeton, NJ/Washington, DC

Details:

<http://www.nerc.com/files/ManagerofCIP.doc>

Policy Analyst

Washington, DC

Details:

http://www.nerc.com/filez/Policy_Analyst.doc

Senior Engineer of Reliability Performance and Events Analysis

Princeton, NJ

Details:

<http://www.nerc.com/files/SeniorEngineerofReliabilityPerformanceandEventsAnalysis.pdf>

Standards Compliance and Regulatory Coordinator

Princeton, NJ

Details:

<http://www.nerc.com/files/StandardsComplianceandRegulatoryCoordinator.pdf>

Subscribe to NERC News:

Send an e-mail message addressed to: subscribe-nercnews@listserv.nerc.com. Leave the subject and body of the message blank.

Unsubscribe from NERC News:

Send an e-mail message addressed to: unsubscribe-nercnews@listserv.nerc.com. Leave the subject and body of the message blank.

Contact NERC at:

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com