NERC Alert System
Overview

Todd Thompson, CIP Investigator
todd.thompson@nerc.net

Chris Lada, Situation Awareness Coordinator
chris.lada@nerc.net
About NERC: Mission

To ensure the reliability of the North American bulk power system

- Develop & enforce reliability standards
- Assess current and future reliability
- Analyze system events & recommend improved practices
- Encourage active participation by all stakeholders
- Pursue mandatory standards across North America
Why Alerts?

- **Events Analysis:**
  - Single event — Based on findings of single event analysis
  - Trends — Multiple events displaying similar causal or contributory causes
  - Generic finding — Equipment or practice showing generic problem
  - Technical finding — Technical analysis reveals potential or repeated problem
Why Alerts?

- Critical Infrastructure Protection & ES-ISAC
- Examples (Not Limited to):
  - US CERT Vulnerability Disclosure
    - e.g. Boreas and ABB alerts
  - Public Vulnerability Disclosure
    - e.g. RealWin SCADA advisory
  - The release of exploitation code or tools
    - e.g. GE Fanuc advisory
  - Release of a malicious code
Purpose

- Provide a secure alert distribution and response system to inform the electric industry of potential reliability vulnerabilities and threats to the bulk power system.
Capabilities

- Notify the entire industry of an alert via email within minutes
- Acknowledge and Respond for multiple entities
- Track acknowledgements, responses, and non-responsive entities
- Upload response documentation, if required or as needed
- Provide flexible user administration for entities
- Automatic reminders for approaching due dates
- **ALL** alert notifications will be sent from: alerts@nercalerts.com

- Users must login to the system to view alerts
  
  - [https://www.nercalerts.com/](https://www.nercalerts.com/)

  - Alerts will **not** be attached or inserted into emails
Alert Type and Handling Levels

**ALERT TYPE**
- Industry Advisory – No Reporting Required
- Recommendation to the Industry – Acknowledgement and Response
- Essential Action Notifications

**HANDLING**
- Public
- Private
- Sensitive
- Confidential
## Handling Provisions

<table>
<thead>
<tr>
<th>Signifier</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Public" /></td>
<td><strong>Public:</strong> No Restrictions.</td>
</tr>
<tr>
<td><img src="image" alt="Private" /></td>
<td><strong>Private:</strong> Restrict to Internal Use and Necessary Consultants / Third-Party Providers</td>
</tr>
<tr>
<td><img src="image" alt="Sensitive" /></td>
<td><strong>Sensitive:</strong> Internal Use Only (Do Not Distribute Outside Your Company)</td>
</tr>
<tr>
<td><img src="image" alt="Confidential" /></td>
<td><strong>Confidential:</strong> Limited Internal Distribution Decided Upon by an Officer of the Company</td>
</tr>
</tbody>
</table>
### Confidential Alerts

**Signifier Requirements**

<table>
<thead>
<tr>
<th>Signifier</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Confidential:</strong> Limited Internal Distribution Decided Upon by an Officer of the Company</td>
</tr>
</tbody>
</table>

- **ONLY** Company Officers and PCCs have the ability to view alerts with ‘Confidential’ Handling Instructions
Company Officer

- Suggested that this person is designated as a company officer or maintains a position of vice president (or equivalent) or higher
- Approve responses and errata

Primary Compliance Contact

- Responsible for timely acknowledgements, responses, and approvals
- May delegate permissions to others, but remains ultimately responsible
- Manage user accounts – add users, remove users, and modify user permissions
- Can assign Company Officers
User Account Roles and Expectations

- **Administrator**
  - Manage user accounts – add users, remove users, and modify user permissions
  - Cannot assign Company Officers

- **“Functional Group” Member**
  - The term “Functional Group” is used to refer to a certain Registered Function (i.e. Transmission Owner) for a given entity
  - Read Alerts
  - Additional permissions can be granted by the PCC or Administrator
Customized Account Permissions

- Additional permissions can be granted at the Entity or Functional Group level.
- Permissions granted at the Entity level apply to all Functional Groups within the entity.
- Permissions granted at the Functional Group level do not apply to the entire entity.
Customized Permissions Hierarchy

Account Permissions

Region Permissions
- Can Acknowledge
- Can Respond
- Cannot Approve

Functional Group Permissions
- Can Acknowledge
- Can Respond
- Can Approve
NERC Alert System
Site Security and Managing Your Account
Login

- Go to https://www.nercalerts.com in your browser and type your email address and password.
- Click the “Forgot your password?” link to have your password sent to you.
- Three incorrect login attempts will lock your account for one hour.
Managing Your Account Information

- Click the “My Account” link to manage your:
  - Contact Information
    - Name
    - Email Address
    - Street Address
    - Phone Number
  - Password
Managing Your Account Information

My Account link
Managing Your Account Information

- Change password
- Update personal information
Website Security

- Encrypted Hypertext Transfer Protocol Secure (HTTPS) communications
- Encrypted database
- Cisco Intrusion Prevention System
- Three failed access attempts cause an account lockout.
- Sessions automatically expire after a period of inactivity or when the browser window is closed.
Physical Security

- Facility access is restricted by keycards.
- Security guards are on-site 24/7.
- Server location is monitored by multiple CCTV cameras.
- Server cabinet is locked, “6-wall” secure.
- Motion-sensitive video camera within server cabinet providing remote viewing.
NERC Alert System
Responding to Alerts
Responding to Alerts – Overview

- Receive the alert email notification.
- **Acknowledge** the alert.*
- **Create** a response.
- If necessary, **edit** the response.
- **Approve** the response.*
- If necessary, update the response with **errata**.

* Required before due date.
A NERC Recommendation to Industry regarding ESP Alert Test has been issued. This Recommendation to Industry applies to Balancing Authority, Generator Operator. The contents of this alert may be specifically useful to individuals with the following responsibilities: Cyber Security - Corporate IT.

An acknowledgment is required within 24 hours of receipt of this notice. Reporting is required by September 30, 2009

To view the alert please log in to the NERC Secure Alert System ([https://www.nercalerts.com/](https://www.nercalerts.com/)) using your assigned username and password.

If you are experiencing difficulties logging in, or cannot find your username or password, please call the help desk @ (866) 972-7192.

Inquiries regarding the subject matter of this Industry Advisory should be directed to:
Go to https://www.nercalerts.com and type your email address and password.
Alert Response Process

- **Required for**
  - Recommendations to the Industry
  - Essential Actions

- **Not Required for**
  - Industry Advisories (Receive/View Only)
- **ALL** alert notification emails will be from: alerts@nercalerts.com

- Users must login to the system to view the alert
## Alert Response Process – Acknowledge

- **Receive Alert Email**
- **Acknowledge Alert**
- **Respond to Questions**
- **Approve Response**
- **Add and Approve Errata**

### Acknowledge for multiple entities

<table>
<thead>
<tr>
<th>Region/Entity</th>
<th>Acknowledgment</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calpine Corporation (FRCC)</td>
<td>By: Admin User on 8/17/2009</td>
<td>Added By: Last Modified By: Approved By:</td>
</tr>
<tr>
<td>Calpine Corporation (MRO)</td>
<td>By: Admin User on 8/17/2009</td>
<td>Added By: Last Modified By: Approved By:</td>
</tr>
<tr>
<td>AES Cayuga (NPCC)</td>
<td></td>
<td>Added By: Last Modified By: Approved By:</td>
</tr>
<tr>
<td>Calpine Corporation (RFC)</td>
<td>By: Admin User on 8/17/2009</td>
<td>Added By: Last Modified By: Approved By:</td>
</tr>
<tr>
<td>Calpine Corporation (SERC)</td>
<td>By: Admin User on 8/17/2009</td>
<td>Added By: Last Modified By: Approved By:</td>
</tr>
<tr>
<td>Ameren - Missouri (AMMO) (SERC)</td>
<td></td>
<td>Added By: Last Modified By: Approved By:</td>
</tr>
</tbody>
</table>

[Back to Alert] [Add Response for Selected]
Alert Response Process – Respond

- Respond to survey questions
- Upload documentation, if required or as needed
- Respond for multiple entities
A Company Officer or their designee must approve a response

Responses must be approved individually
‘Errata’ allows you to change or clarify your response to the alert

Errata must be re-approved by a Company Officer or their designee
Viewing the Response Status

- View the status of an alert at any time.
- The site tracks:
  - when an alert was acknowledged and which user acknowledged it.
  - when a response was added and edited and which user modified it.
  - when the response was approved and which user approved it.
Viewing the Response Status

Click the Status button.
Viewing the Response Status

Acknowledgement Status
(Acknowledged)

Response Status
(Approved)

Response Status
(Not approved)
Status Report

- Who and When:
  - Acknowledged an alert
  - Last updated a response
  - Approved a response

- Summary of alert status for user entities
Sample Recommendation

Recommendation to Industry
Band of Desert Dwellers

Distribution Date: August 08, 2009

Status:

Acknowledgment Required by August 25, 2009
Response Required by August 27, 2009

PRIVATE: RESTRICT TO INTERNAL USE AND NECESSARY CONSULTANTS/THIRD-PARTY PROVIDERS

Instructions:

This NERC Recommendation is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Recommendation. However, pursuant to Rule 810 of NERC’s Rules of Procedure, you are required to report to NERC on the status of your activities in relation to this recommendation. For U.S. entities, NERC will compile the responses and report them to the Federal Energy Regulatory Commission.

Issuance of this Recommendation does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Recommendation if such failure constitutes a violation of a Reliability Standard.

Distribution:

Regions:
All Regions
Site Help Contents

- Step-by-step instructions for:
  - Managing and responding to alerts
  - Creating and configuring user accounts
- Frequently Asked Questions
- Help Desk Contact Information
Accessing the Site Help

Login and click Help.
Help Desk Support

- Contacting the Help Desk
  - Phone: (866) 972-7192
  - Hours: Weekdays from 08:00 to 17:00 Central

- Help Desk is available to
  - Provide user assistance
  - View your entity membership and permissions
  - Unlock accounts

- Cannot answer questions about specific alerts or change your permissions
Questions?

Todd Thompson, CIP Investigator

todd.thompson@nerc.net

Chris Lada, Situation Awareness Coordinator

chris.lada@nerc.net