

**Business Casual Attire**

# NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

## Critical Infrastructure Protection Committee

Wednesday, March 15, 2006 — 9 a.m. to noon (Joint with PC and OC)

Thursday, March 16, 2006 — 8 a.m. to 5 p.m.

Friday, March 17, 2006 — 8 a.m. to noon

Phoenix Marriot Mesa  
200 N. Centennial Avenue  
Mesa, Arizona

***(PLEASE BE PREPARED TO STAY FOR THE ENTIRE MEETING.)***

## Meeting Agenda

### 1. Administrative Matters (30 minutes)

- a) Arrangements — Stan Johnson
- b) Announcement of quorum — Stan Johnson
- c) Procedures — Stan Johnson
- \*d) NERC Antitrust Compliance Guidelines — Stan Johnson
- e) Parliamentary procedures — Stan Johnson
- f) Introduction of members, alternates, and associates — Stan Johnson
- g) **Approval** of agenda — Barry Lawson
- \*h) **Approval** of December 8–9, 2005 CIPC meeting minutes — Barry Lawson

### 2. Information Items

- a) CIPC Executive Committee report — Barry Lawson (**10 minutes**)
  - 1. Electricity Sector Coordinating Council update
    - a. NIPP discussion
    - b. Scheduling ESCC-GCC meeting for late April
- b) NERC report — Lou Leffler (**20 minutes**)
- c) ESISAC report — Lou Leffler (**20 minutes**)
  - 1. Exercises Update
    - \*a. Cyber Storm — Lou Leffler
    - b. Blue Cascades III — Stan Johnson
- d) Electric Reliability Organization formation process update — Gerry Cauley (**45 minutes**)

A New Jersey Nonprofit Corporation

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

- e) Working groups and task force 2006–2007 plans (**30 minutes**)
  - 1. CIPC Organization Review — Stan Johnson
  - 2. Brief update of current activities — working group/task force Chairs

### 3. Security Planning

- a) Cyber Security Standards: CIP-002-1–009-1 — Larry Bugh (**15 minutes**)
- b) Outreach Working Group — Walter Johnson (**60 minutes**)
  - 1. CIP-002-1–009-1 workshops
- c) Control System Security Working Group — Tom Flowers (**20 minutes**)
  - 1. CSSWG Update
    - a. Information security
    - b. Zero Day event detection
    - c. Incident response
  - \*2. Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations – 2006 (expected to be presented for approval)
  - 3. “Roadmap to Secure Control Systems in the Energy Sector” — Hank Kenchington  
**Link:** <http://www.controlsystmsroadmap.net> (**45 minutes**)
    - a. Overview of the Roadmap
    - b. At the June meeting, the CIPC Executive Committee will be asking members to:
      - endorse the Roadmap document
      - endorse that the CIPC Executive Committee provide oversight regarding the implementation and evolution of this document, through its role as the Electricity Sector Coordinating Council
  - 4. SCADA Summit–review and potential initiatives — Mike Assante

### 4. Security Operating

- a) Indications, Analysis, Warnings Working Group — Larry Bugh (**5 minutes**)
  - 1. Program review
- b) Reporting Technology Working Group — Carl Eng and HSIN developers (**60 minutes**)
  - \*1. Review Homeland Security Information Network (HSIN) documentation
    - \*a. Memorandum of Understanding between DHS and NERC
    - \*b. Registration End User Agreement
  - 2. Set the path forward to establish approval process to proceed with HSIN-ES implementation
- c) 2005 Hurricane Season Lessons Learned (**45 minutes**)
  - 1. Ron Landry — Lafayette Utilities
  - 2. Stan Johnson — [Report on DOE conference](#)
- d) Power Down at Primary Control Center — Tom Glock (**15 minutes**)
- e) Influenza Pandemic — Stan Johnson (**15 minutes**)

### 5. Agency Reports (30 minutes)

- a) Department of Homeland Security
- b) Department of Energy
- c) Public Safety Canada
- d) Federal Energy Regulatory Commission

## 6. Closing

- a) Follow-up items and future actions — Barry Lawson (**10 minutes**)
- b) Future meetings — Stan Johnson

### **2006**

- June 21–22, Washington, D.C.
- September 13–15, Boston, Massachusetts (with AGA/EEI)
- December 6–8, Houston, Texas or Tampa, Florida (with NERC)



## **NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL**

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

### **NERC ANTITRUST COMPLIANCE GUIDELINES**

#### **I. GENERAL**

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

#### **II. PROHIBITED ACTIVITIES**

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

Approved by NERC Board of Trustees, June 14, 2002  
Technical revisions, May 13, 2005

### III. ACTIVITIES THAT ARE PERMITTED

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

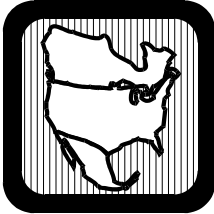
In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.



## **NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL**

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

### **Critical Infrastructure Protection Committee Meeting**

December 8–9, 2005  
St. Petersburg, Florida

#### **Draft Minutes**

A regular meeting of the Critical Infrastructure Protection Committee (CIPC) was held on December 8–9, 2005 in St. Petersburg, Florida. The meeting notice, agenda, and attendance list are affixed as **Exhibits A, B, and C**, respectively. Meeting presentations that are publicly available may be found at: <http://www.nerc.com/~filez/cipmin.html>.

Chairman Stuart Brindley presided.

Secretary Stanley Johnson announced that a quorum was present and confirmed the following proxies:

- 1) Joe Doetzl for Larry Dolci.
- 2) Michael Brytowski for Dave Kulissek
- 3) Kurt Muehlbauer for Linda Nappier
- 4) James Strange for Mike Hyland
- 5) Mike Knauer for Bob Richhart

#### **Antitrust Guidelines**

The secretary reviewed the NERC Antitrust Compliance Guidelines.

#### **Introductions**

The committee members and guests introduced themselves.

#### **Logistics**

The secretary reviewed the meeting arrangements, site requirements, and agenda adjustments.

#### **Parliamentary Procedures**

The secretary reminded the attendees of the use of proper parliamentary procedures and the scheduled election of four members of the CIPC Executive Committee for 2006–2007.

#### **Agenda**

The CIPC members approved the meeting agenda moved by Eric Solberg, seconded and passed with no dissenting votes.

## **Minutes**

The CIPC members approved the minutes of the September 29–30, 2005 meeting, moved by Tom Bowe, seconded and passed with no dissenting votes.

## **CIPC Nominating Task Force Report**

Roger Lampila presented the report from the Nominating Task Force. He presented the nomination of four nominees to the CIPC Executive Committee for the 2006–2007 term. The nominees were Larry Bugh, Bob Canada, Tom Glock, and Roger Lampila.

## **Election of CIPC Executive Committee**

Roger Lampila moved the nominating committee slate. Additional nominees were solicited from the floor and none were received. The slate was approved unanimously. The CIPC Executive Committee for the next two years is listed below:

CIPC Chair:	Stuart Brindley
CIPC Vice Chair:	Pat Laird
CIPC Vice Chair:	Barry Lawson
Cyber Security:	Larry Bugh
Physical Security:	Bob Canada
Operations:	Tom Glock
Policy:	Roger Lampila
Secretary:	Stan Johnson

## **CIPC Executive Committee Report**

Stuart Brindley reported that work continues on development for private-sector government collaboration using the proposed legal framework on the sector partnership model. The Electricity Sector Coordinating Council (ESCC) had previously been appointed and meets with the Government Coordinating Council.

CIPC membership for the period January 2006 through December 2007 is under review by the NERC Regional Managers and the designated Associations.

The ESCC had submitted comments on the draft Energy Sector Specific National Infrastructure Protection Plan (NIPP) in its July 22, 2005 letter to DOE. DHS since issued the draft Base NIPP and individuals have submitted comments. In general, electricity sector concerns with the draft Base NIPP include excessive detail, unsubstantiated need for certain specific information such as critical assets and vulnerability assessments, and insufficient focus on mitigation and recovery segments of security planning. A final opportunity to comment on the revised Base NIPP will be provided during a two-week period in early 2006.

Larry Bugh reviewed the NERC Board of Trustees meeting of November 1, 2005.

## **NERC Report**

Lou Leffler reviewed recent activities at NERC. Current focus and resources are being applied to the Electric Reliability Organization (ERO) application and the technical conferences conducted by the U.S. Federal Energy Regulatory Commission (FERC). (See item below)

## **Electricity Sector Information Sharing and Analysis Center (ESISAC) Report**

Lou Leffler reviewed the recent activities of the ESISAC.

Work continues with the Telecommunications Electric Power Interdependency Task Force (that reports to the National Security Telecommunications Advisory Committee) regarding the mutual interdependencies including priority restoration issues.

The National Infrastructure Advisory Council's Intelligence Coordination Study Group is working with many intelligence agencies and private sectors to determine the needed information input, including subject matter expertise, to the agencies, the requisite security information to the private sectors, and the most effective enabling mechanisms. The Homeland Security Information Network (HSIN) is considered to be a primary (among others) communications vehicle.

Bulk electric system situational awareness is becoming key to work in the sector for the government agencies and the sector entities. Much work is yet to be done regarding what awareness is required, from whom, to whom, mechanisms, frequency, and timeliness.

The Electronic Tagging incident that occurred in August 2005 has been studied and a report prepared (with the significant support of Jeff Dagle) for the electricity sector

The Department of Homeland Security (DHS) exercise Cyber Storm will be conducted in February 2006. Several electricity sector entities will participate.

### **Electric Reliability Organization Formation Process Update**

Gerry Cauley presented a thorough update on the status of the ERO development. Key to CIPC are the expected needs for bulk electric system situational awareness, infrastructure security, event analysis, and information sharing. Technical expertise will be required to develop solutions in these areas.

### **Working Group/Task Force Organization and Procedures**

The CIPC Working Group and Task Force Organization and Procedures document was moved by Stuart Brindley, seconded and approved by CIPC as amended. The amended version is attached to these minutes as **Exhibit D**. The amended version was created after some clarifying discussion about the roles and responsibilities of the working group and task force chairs.

### **Working Group and Task Force 2006–2007 Plans**

The chairs of the working groups and task forces presented a brief summary of their groups.

### **Critical Spares Task Force**

Stan Johnson reported Phil McCrory of TXU is now the chair of the task force. The task force is inactive and should be temporarily suspended as it has not met for over eighteen months. The primary focus at this time is the Spare Equipment Database (SED) and keeping it operational. NERC staff IT professionals are responsible for this function. The Edison Electric Institute Spare Transformer Equipment Program (STEP) is gaining momentum and 2006 will determine more clearly the direction for spare equipment.

### **Risk Assessment Working Group**

Ted Heller presented a brief update and offered the working group's assistance for the implementation of CIP-002.

## **Security Guidelines Working Group**

Seiki Harada reported on the reorganization of the working group and the 2006/2007 action plan. He will be transitioning the leadership of the group to Scott McCoy.

## **Cyber Security Standards**

Larry Bugh updated CIPC on the permanent cyber security standards known as CIP-002-1 through CIP-009-1. The drafting team has been working with great diligence to respond to comments provided by the electricity sector. The current plan is to post for the 30 day pre-ballot period on January 16, 2006. The initial ballot will commence February 15, 2006. Given final approval by the ballot body, the NERC Board of Trustees will be asked to adopt the standards at their meeting on May 2, 2006, with an effective date of June 1, 2006. The implementation plan details the expected times for compliance over the next several years. CIPC members were encouraged to become advocates for the standards.

## **Outreach Working Group**

Wally Johnson reported on the working group deliberations regarding the very important outreach required to support implementation of the permanent cyber security standards. This is considerably more comprehensive than the outreach done for the Standard 1200. The program is currently being designed. The steering committee for this outreach has requested support from the Standard 1200 Education Team, the Cyber Security Standard Drafting Team, and others. Outside support may also be recommended on a cost recovery basis.

## **Control Systems Security**

Tom Flowers presented the Control Systems Security Working Group work plan for 2006. Tom moved for approval, it was seconded and CIPC approved this document with recognition that the active participants list is being updated.

The Potential Mitigations Strategies for the Common Vulnerabilities of Control Systems were presented. Tom moved its approval as a reference document. It was seconded and approved by CIPC. The mitigations for each of the ten vulnerabilities are described as foundational, intermediate, and advanced. This work will be given wide dissemination within the electricity sector and will be a publicly available document. The working group is now engaged in developing an update of this ongoing document.

Electricity sector entities engaged in the security of control systems are encouraged to consider participation in the 2006 SCADA Security Summit, March 1–3, 2006 in Orlando, Florida.

## **Indications, Analysis, and Warning Working Group**

Larry Bugh reported that the updated Indications, Analysis, and Warning program document, approved by CIPC in September, has been signed by NERC and the U.S. DHS. This working group's work plan is expected to be presented to CIPC for the June 2006 meeting.

## **Homeland Security Information Network (HSIN)**

Julie Silberger, Carlos Kizzee, Patrick Ansaldi, and Greg Holland, representatives of the DHS, updated the current project status. The DHS and NERC are developing a memorandum of understanding regarding how HSIN submissions will be protected. An end user agreement is also being written to guide HSIN users. The laws were explained including the exemptions to FOIA, the passing of submitted information to other agencies, recurring submissions, and submitter control of input and subsequent use thereof. The intent is to finalize all documentation, mechanics, and user registration process for formal approval at the March 2006

CIPC meeting. Following that, the HSIN implementation including registration and training will proceed. There will be a logical tie between the Reliability Coordinator Information System and HSIN, for HSIN information only, to facilitate use by the reliability coordinators. CIPC gave a general indication that the approach appears on track and will take action as indicated. HSIN will be used during the Cyber Storm exercise.

### **Ground Truth Task Force Authorized**

The Executive Committee authorized a task force to lead the “ground truth” initiative and to support the Risk Assessment Working Group and the Control Systems Security Working Group. The “ground truth” initiative is intended to determine the implications to the electricity sector of attacks on the bulk electric system control systems. Roger Lampila will chair the task force that will develop a scope to include the expectations for the project, collaboration with the NERC Operating Committee, and studies with asset owners and operators, and the involved National Laboratories.

### **Crisis Response Task Force**

Tom Bowe reported that a standard operating procedure to support the ESISAC will be presented to the CIPC for the March 2006 meeting.

### **Laptop and Handheld Computer Thefts**

Seiki Harada and Dave Baumken made presentations based on their experiences with laptop thefts. A reference document that included good practices for consideration by the electricity sector has been prepared and is attached to these minutes as **Exhibit E**. The document will be distributed to the electricity sector and to other critical infrastructure Information Sharing and Analysis Centers (ISACs)

### **Cyber Intrusion Detection Systems**

Rob Walters, EWA-Canada and George Bakos, Dartmouth College reported on the conclusions of a pilot project conducted during the past year involving several ISOs to evaluate IDS tools and analytical capabilities.

### **Contagious Disease Pandemic Preparedness**

Stan Johnson reported on the proposed reference guide. The guide has been prepared to assist the electricity sector in enhancing its business continuity planning in light of the threat posed by the Avian flu occurring in Asia. The document will be submitted to CIPC for email ballot in January, followed by subsequent distribution to the electricity sector.

### **Agency Reports**

*U.S. Department of Homeland Security* (DHS) — Paul Carrier presented an update. He reported reorganization is under way in the department but the implications for the electricity sector are minimal. He reviewed the Base NIPP development schedule and the sector specific NIPP development schedule.

*U.S. Department of Energy* (DOE)— Matt Rosenbaum presented a few brief remarks.

*Public Safety Emergency Preparedness Canada* (PSEPC) — Joan Eagan made an interesting presentation on the PSEPC’s Strategy Development process. Extensive work has been done to collect input from the public, private sector, and the government agencies. The “all threats” approach is based on information sharing and good planning. (Presentation is posted on the NERC Web site)

*Federal Energy Regulatory Commission* (FERC) — Regis Binder presented an update. He discussed the commission's progress in complying with the Energy Policy Act of 2005 and its process for establishing the Electricity Reliability Organization.

### **Round Table**

Mike Peters has been appointed to the key Cyber Security position at the U.S. FERC. Mike encouraged CIPC members who used the security information distributed at the September CIPC meeting to send a note of appreciation to Paul Carrier or Hank Kenchington.

Dave Norton offered to present a lessons learned from Hurricane Katrina at the next CIPC meeting.

### **Appreciation**

CIPC expressed its appreciation to Jamey Sample for his service on the CIPC Executive Committee.

CIPC expressed its appreciation Ted Heller for his leadership in development of the NERC reference document: Risk-Assessment Methodologies for Use in the Electric Utility Industry.

### **Closing**

Chairman Brindley closed the meeting at 11:00 am on December 9, 2005.

### **Future Meetings**

#### **2006**

- 1) Thursday (8 a.m. to 5 p.m.) – Friday (8 a.m. to noon), March 16–17, 2006; Mesa, Arizona (coupled with NERC standing committees and AGA/EEI Security Committee).
- 2) Wednesday (8 a.m. to 5 p.m.) – Thursday (8 a.m. to 5 p.m.), June 21–22, 2006; Washington, DC (to include cleared briefing with DHS).
- 3) Thursday (8 a.m. to 5 p.m.) – Friday (8 a.m. to 5 p.m.), September 14–15, 2006; Cambridge, Massachusetts (possibly coupled with NERC standing committees and possibly with AGA/EEI Security Committee).
- 4) Thursday (8 a.m. to 5 p.m.) – Friday (8 a.m. to noon), December 7–8, 2006; Tampa, Florida or Houston, Texas (coupled with NERC standing committees).

Respectfully submitted,

Stanley L. Johnson  
NERC Staff

## **CYBER STORM EXERCISE**

The Department of Homeland Security (DHS) National Cyber Security Division conducted the Cyber Storm exercise during the week beginning February 6, 2006. The basic DHS exercise description is attached. Planning commenced in the spring of 2005. Several Electricity Sector (ES) entities were involved in the actual exercise as players in their operational locations. Some of the ES entities participated at the Exercise Control Center. The ES participants were anonymized during the exercise. The exercise contained several challenges throughout the week with events leading up to zero day, during that day, and somewhat beyond. The incidents were not designed to really challenge cyber systems; the intent of the exercise was to test communications and response to serious cyber events.

In addition to the ES, other participants were representing several federal agencies (including DHS and the Department of Energy), international including substantial Canadian participation (including Public Safety Emergency Preparedness Canada), information technology, state and local, transportation, communications, law enforcement and intel.

The ES participants simulated two Reliability Coordinators, four Transmission Operators, one Load Serving Entity, and the ES Information Sharing and Analysis Center (ESISAC). Several other ES participants were engaged primarily through information sharing.

The “attacks” were induced by organizations seeking to make publicity for their causes. The cyber attacks resulted in loss of information and system interruptions. There was no intent to suggest that the attack vectors were valid or that they could induce the damage done; again, the intent was to test communications and response.

There have been several after action meetings to discuss results. A formal DHS report will be completed by May 2006. Participants generally found the exercise to be useful in generating lessons learned. The ESISAC conducted an after action discussion and the following page includes comments. It is worth noting that one of our communications mechanisms was the Homeland Security Information Network (HSIN). We developed a good list of learnings. Before the exercise we conducted three webex/conference calls on use of HSIN; this will help in establishing HSIN for the entire ES, given CIPC approval.

One little side note; in these exercises there is a complete glossary of terms including:

STARTEX: Start.

EXPLAN: Exercise Plan.

MSEL: Master Scenario Events List.

ENDEX: Exact date and time exercise ends (we were all happy when ENDEX came!).

HOT WASH: The discussions of lessons learned following ENDEX.

And, finally we all learned that you don't even think of talking or writing about this until you state, “Exercise – Exercise – Exercise”.

# **CYBER STORM EXERCISE**

## **SOME LEARNINGS BY THE**

### **ELECTRICITY SECTOR INFORMATION SHARING AND ANALYSIS**

#### **CENTER**

**(For discussion; not in any priority order.)**

1. Communications
  - A. Voice
    - a. Need assurance of backup communications:
      - i. Cell phones
      - ii. Satellite phones
      - iii. Radio
    - b. Critical Infrastructure Warning Network (CWIN) was used by the two connected Reliability Coordinators (RC) and the Electricity Sector Information Sharing and Analysis Center (ESISAC). Need to complete the program for all RCs.
    - c. Conference call arrangements:
      - i. Security Briefing groups
      - ii. Inter-ISAC
      - iii. Ad hoc groups as needed
      - iv. Can be arranged by ESISAC or (upon request) by NICC. ESISAC will likely use the anytime available capability.
    - d. Consider deployment of an emergency notifications system (“push communications”).
  - B. Email
    - a. Use of email is tenuous in assurance of message delivery in time of stress.
    - b. Multiple listservs resulted in several duplicate messages. While better to over-communicate than under, better yet to focus the electronic communications.
    - c. Use crisp, definitive subjects in emails.
    - d. Consider email protocol, e.g. reply to sender vs reply to all.
  - C. Homeland Security Information Network – Electricity Sector (HSIN-ES)
    - a. HSIN was used extensively for incident reporting (in the CIPIS function) and for Urgent Alerts.
    - b. Enlarge the Urgent Alert section of the HSIN homepage.
    - c. Need emails from HSIN/CIPIS sent to ESISAC Staff.
    - d. HSIN / CIPIS reports sent must appear in the senders’ all and sent boxes.
    - e. Other mechanics to ease use will be implemented.
  - D. Trim up all communications, to make sure the messages are sent, received, and not unnecessarily duplicated.
  - E. Know the communications mechanisms; practice them.
2. Discussions to be held with agencies on how to improve communications: content and to whom.
3. Consider, with DOE, revision to the Form-417 and mechanics with inclusion in HSIN.
4. Stress essential requirement that request for information (RFI) communications route through ESISAC, to avoid extra communications, especially with operators engaged in monitoring and restoration. Worked well during exercise.
5. Set up standard RFI formats for events such as hurricanes, outages, attack (physical or cyber), and utilize in HSIN collaboration tool.
6. RFIs that lead toward detail analysis and forensics should be treated as post-event activities. During the event focus must remain on continued situational awareness, recovery, and determination of essential causation to mitigate during the ongoing event. Forensics preservation is a critical part of ongoing functions.

7. Continue to work toward bulk electric system INFORMATION to agencies, based upon DATA analyzed by Electric Sector, with ESISAC support. Continue to develop useful tools (for example) NESEC, Frequency and ACE, PMU Project.
8. Need method for determining the change of the cyber and physical threat alert levels for the Electricity Sector.
9. Need more ESISAC staff in an emergency. Would form team similar to the 14 August outage, and should be pre-organized and practiced. Tasks would include: communications, data gathering, analysis, subject matter expertise gathering.
10. Connectivity between DHS-NICC and US-CERT was not clear.
11. Need clarity in the naming of Energy Sector and Electricity Sector and the Energy ISAC and Electricity Sector ISAC.
12. Participants were anonymized during the Cyber Storm exercise. This posed difficulties in analysis on a large scale basis (understood for the exercise). Need good situational awareness (including, for example, maps) for actual events.

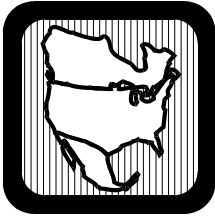


# Homeland Security

## Cyber Storm 2005

### Key Messages

- Cyber Storm is a nationwide cyber security exercise that is intended to act as a catalyst for assessing communications, coordination, and partnerships across the public and private sectors in the event of a cyber attack. Cyber Storm is the first cyber exercise testing response across the private sector as well as international, federal, and state governments.
- Cyber Storm is led by the Department of Homeland Security and coordinated by its National Cyber Security Division (NCSD).
- The exercise examines how best to communicate, coordinate a response, assess secure communication channels, and identify recovery mechanisms to a campaign-level cyber attack. Cyber Storm is part of an ongoing effort of studies and analyses to improve rapid response and cyber security.
- Cyber Storm supports the National Strategy to Secure Cyberspace by testing national cyber security response efforts and providing critical input to the development of a National Cyber Security Response Plan.
- Cyber Storm is in accordance with FY 05 congressional appropriations to conduct exercises that test the response to cyber attacks on critical infrastructures.
- Cyber Storm scenarios are simulations using fictitious technical vulnerabilities and threats and does not by any means affect cyberspace or the Internet. The benefits of this strategy include:
  - Preventing disclosure of real vulnerabilities during and after the exercise
  - Encouraging participants to focus on communications and coordination by eliminating diversions in searching for technical solutions.
- Cyber Storm is a collaborative effort and includes robust participation by the private sector, as well as federal, state, and foreign allied governments.



## **NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL**

---

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

### **TOP 10 VULNERABILITIES OF CONTROL SYSTEMS AND THEIR ASSOCIATED MITIGATIONS – 2006**

**North American Electric Reliability Council  
Control Systems Security Working Group**

**U.S. Department of Energy  
National SCADA Test Bed Program**

**February 28, 2006 (Draft)**

#### **Preamble**

This document addresses potential risks that can apply to some electricity sector organizations and provides practices that can help mitigate the risks. Each organization decides for itself the risks it can accept and the practices it deems appropriate to manage its risks.

#### **Introduction**

This reference document provides a non-prioritized list of the top 10 most common and threatening vulnerabilities to control systems in the Electric Sector based on the combined expertise on the NERC Control System Security Working Group (CSSWG) members. This list is prepared by the CSSWG and updated annually. Asset owners are encouraged to use this list to augment their risk management processes.

The U.S. Department of Energy National SCADA Test Bed (NSTB) Program has provided initial recommended mitigation strategies to the list of vulnerabilities prepared by the CSSWG members. Three levels of mitigation strategies – *foundational*, *intermediate*, and *advanced*, are proposed. *Foundational* strategies are considered to be minimal mitigation strategies typically involving the establishment of security policy and fundamental implementations. *Intermediate* strategies are a next step in establishing a secure posture and involved readily available technologies or the stronger implementation of baseline policies. *Advanced* mitigation strategies provide long term achievable security posture guidance but may include tools or technologies that are currently not readily available.

## **Top 10 Vulnerabilities of control systems and potential mitigation strategies**

### **1. Inadequate policies, procedures & culture governing control system security.**

#### **Mitigation Strategies:**

- Foundational
  - The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards (CIP-002 through CIP-009). (CIP-003-1 R2)
  - Develop and implement policies and procedures with executive level buy-in, including the NERC critical infrastructure protection standards, which govern control system security.
  - The Responsible Entity shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Infrastructure Assets.
  - Provide basic security awareness training for all employees. (CIP-004 R1 & R2)
- Intermediate
  - Senior manager providing periodic briefings to executive management detailing control system risk posture.
  - Share industry “best practices” in security policy structure and topics.
  - Provide periodic computer based control system cyber security training for all control systems personnel.
  - Provide social engineering awareness training for all employees.
- Advanced
  - Adopt a process for continuous improvement for implementation and enforcement of policies and procedures governing control system security.
  - Provide periodic hands-on cyber-security training for control systems personnel taught by applicable vendor or consulting firm.
  - Perform periodic security awareness drills and audits.

### **2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms.**

#### **Mitigation Strategies:**

- Foundational
  - Control system stakeholders and designers demanding security solutions from vendors.
  - Detailed security requirements included in all design specifications.
  - Implement electronic perimeters. Disconnect all unnecessary network connections, following the NERC security guideline called Control System — Business Network Electronic Connectivity Guideline. (Also addressed in NERC CIP-005.)
  - Access controls can be considered part of an organization’s defense in depth solution. (CIP-005 R2, CIP-007 R5)
- Intermediate
  - Existing standards and best practices referenced as requirements in design specification.

- Implement concentric electronic perimeters. Use autonomous networks with minimal shared resources between control system and non-control system networks.
- Distribute the organization's practices and guidelines to employees, vendors, and integrators as part of training & refresh cycle.
- Advanced
  - Design specifications including a comprehensive security standard references providing in-depth security coverage.
  - Implement virtual local area networks (VLANs), private VLANs, intrusion prevention, anomaly detection, smart switches, secure dial-up access, etc.
  - Endpoint security software.

### **3. Remote access to the control system without appropriate access control.**

#### **Mitigation Strategies:**

- Foundational
  - Policy in place for managing user access.
  - The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). (CIP 002-009).
  - Complete maps of system topology maintained and all access points identified with up to date status.
  - Perform background personnel checks on employees with access to sensitive systems. Ensure vendors and contractors have implemented similar procedures. (CIP-004 R3)
  - Establish a policy for system access including password authentication. (CIP-005 R5)
  - Change all default passwords where possible. (CIP-005 R4)
  - Do not allow unsecured modems.
  - Use VPN technology when the Internet is used for sensitive communications.
  - Follow the NERC security guideline called Securing Remote Access to Electronic Control and Protection Systems. (CIP-005)
- Intermediate
  - Define levels of access based on need. (CIP-007) Assign access level and unique identifiers for each operator. (Implied by CIP-007) Log system access at all levels. (CIP-007) Implement a network intrusion detection system to identify malicious network traffic, scan systems for weak passwords, separate networks physically. (Partially covered in CIP-007.)
  - Make contractual agreements for vendor access to control system components a requirement in RFPs.
  - Isolate user access to compartmentalized areas based on specific user needs.
- Advanced
  - Automated removal of user accounts tied to badge systems or human resources employee termination.
  - Design access levels into the system restricting access to configuration tools and operating screens as applicable. Segregate development platforms from run-time platforms. Use multifactor authentication (e.g., two-factor, non-replayable credentials). Implement protocol anomaly-detection and active-response technology.

#### **4. Auditable system administration mechanisms (system updates, user metrics, etc.) are not part of control system implementation.**

##### **Mitigation Strategies:**

- Foundational
  - Periodic configuration auditing and backup.
  - The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets.
  - Establish required metric for vendor update support of security patches as part of RFP. Maintain a maintenance agreement with software vendors for update notification and distribution. Define change-management process. (CIP-003)
- Intermediate
  - The development system maintained for testing system updates prior to operational system deployment when appropriate.
  - Establish a schedule of checks for system updates for all applicable software, operating systems, and component firmware. Implement version control system and enforce change-management process. (CIP-007)
- Advanced
  - Phase out obsolete, non-maintained legacy systems.
  - Utilize a dual-redundant or clustered system architecture that allows for re-bootable updates without requiring system downtime. Security scan resources to ensure security patches are installed. (Caution: Procedures should be developed to ensure online control systems are not compromised as a result of the scan).

#### **5. Inadequately secured wireless communication.**

##### **Mitigation Strategies:**

- Foundational
  - Periodic risk assessment of all wireless implementations including Denial of Service.
  - All wireless connections treated as remote access points.
  - Establish a policy on where wireless may be used in the system.
  - Implement encrypted wireless communication where possible (e.g. wired equivalent privacy [WEP]).
- Intermediate
  - Authenticated control signals.
  - Implement 802.1x device registration.
- Advanced
  - For 802.11:
    - Implement wireless fidelity protected access (WPA) encryption.
    - Use non-broadcasting server set identifications (SSIDs).
  - Implement 802.11i.
  - Use public key infrastructure (PKI) and certificate servers.
  - Utilize media access control (MAC) address restrictions.
  - Implement 802.1x device registration along with unregistered device detection.

**6. Use of a non-dedicated communications channel for command and control, such as Internet based SCADA, and/or inappropriate use of control system network bandwidth for non-control purposes (e.g. VOIP).**

**Mitigation Strategies:**

- Foundational
  - Define critical network paths. (CIP-003)
  - Restrict or eliminate non-critical traffic on the control network and ensure quality of service for all control system traffic.
  - Segregate functionality onto separate networks (e.g., do not combine e-mail with control system networks).
- Intermediate
  - Implement intrusion detection to monitor traffic. Evaluate network traffic and control system point counts and polling rates. Reconfigure for optimal use of existing resources.
- Advanced
  - Update system technology to allow for higher bandwidth traffic. Separate critical and non-critical systems. Implement protocol anomaly systems to enforce legitimate traffic.

**7. Lack of quick and easy tools to detect and report on anomalous or inappropriate activity. Inadequate or non-existent forensic and audit methods.**

**Mitigation Strategies:**

- Foundational
  - Network traffic periodically audited against policy. System logs, where available, regularly audited.
  - System logs and sequence of events recorders time synchronized with GPS clocks or network time protocol (NTP).
  - Install monitoring technology to log all existing and potential points of entry into the system. Preserve logs for subsequent analysis.
- Intermediate
  - Implement technologies to enforce legitimate traffic.
  - Install anomaly detection where available. Actively monitor logs.
- Advanced
  - Implement tamper resistant/proof long term storage for all forensic data.
  - Introduce SCADA/Control System protocol signatures when they become available.
  - Work with vendors to develop appropriate tools to identify inappropriate control systems traffic.

**8. Installation of inappropriate applications on critical control system host computers.**

**Mitigation Strategies:**

- Foundational
  - Identify/develop policy that will provide guidance for allowable applications and their introduction onto the SCADA/Control System LAN. (CIP-005)

- Conduct inventory. Ensure sufficient training of personnel responsible for component configuration and maintenance.
- Intermediate
  - Implement mal-ware detection. (CIP-007)
- Advanced
  - Anomaly detection can be used to detect inappropriate applications.
  - Develop application baseline profile for each workstation and server on control network. Configure intrusion detection filters to identify and log baseline violations.

## **9. Software used in control systems is not adequately scrutinized.**

### **Mitigation Strategies:**

- Foundational
  - Develop and implement software lifecycle policy: The policy identifies how new software is acquired including the purchasing and review process. It also defines how updates are managed and how antiquated software is retired.
  - Risk assessment & software quality control required on new and existing systems.
- Intermediate
  - Evaluate and characterize applications. Remove or disconnect unnecessary functions.
  - Evaluate the patch management process, including hardware, firmware, and software, following the NERC security guideline called Patch Management for Control Systems.
  - Maintain full system backups and have procedures in place for rapid deployment and recovery. Maintain a working test platform and procedures for evaluation of updates prior to system deployment.
  - Build security into applications during system design to include the ability to validate new code releases and to authenticate the code source.
- Advanced
  - Source code and development tool review.
  - Systematic search for additional vulnerabilities.

## **10. Control systems command and control data not authenticated.**

### **Mitigation Strategies:**

- Foundational
  - Limit connections and isolate control systems communications and networking infrastructure.
  - Identify the different types of SCADA/Control Systems. Determine which data sets need to be authenticated and protected for integrity.
- Intermediate
  - Basic data authentication/integrity.
  - If used or where possible key management policies and systems in place based on an agreed set of standards, procedures, and secure methods for all issues (e.g. usage, storage, revocation, logging, auditing, etc.) associated with use of keys.
- Advanced

- Authenticate and validate control system communication with integrity protection.
- Utilize SCADA/Control Systems protocols that contain authentication and integrity attributes.

# Memorandum of Understanding

between

**The United States Department of Homeland Security**

and

**The North American Electric Reliability Council**

concerning

**The Homeland Security Information Network-Electricity Sector**

## I. Parties to the Agreement

This Memorandum of Understanding (MOU) is entered into between the Department of Homeland Security (“the Department” or “DHS”) and the North American Electric Reliability Council<sup>1</sup> or any successor entity as representing the interests of the Electricity Sector Coordinating Council (“the Sector” or “the ESCC”) where the ESCC is recognized by the Department as an Information Sharing and Analysis Organization<sup>2</sup>.

## II. Electricity Sector

The Electricity Sector (ES) is comprised of thousands of electric utilities (cooperatives, federal power agencies, investor owned, municipals) in the United States and Canada. Supporting the ES in the security area are the North American Electric Reliability Council (NERC), the Critical Infrastructure Protection Committee (CIPC), the Electricity Sector Coordinating Council (ESCC), and the ES Information Sharing and Analysis Center (ESISAC).

- A. NERC. The NERC's mission is to ensure that the bulk electric system in North America is reliable, adequate and secure.

---

<sup>1</sup> The NERC is a nonprofit New Jersey corporation whose members are eight regional reliability councils. The members of these councils come from all segments of the electric industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal and provincial utilities; independent power producers; power marketers; and end-use customers. These entities account for virtually all the electricity supplied and used in the United States, Canada, and a portion of Baja California Norte, Mexico. NERC's mission is to ensure that the bulk electric system in North America is reliable, adequate and secure. Since its formation in 1968, NERC has operated as a self-regulatory organization, relying on reciprocity, peer pressure and the mutual self-interest of all those involved in the production, transmission, and distribution of electricity in North America.

<sup>2</sup> An Information Sharing and Analysis Organization is defined within 6 C.F.R. § 29.2 as a, “...*formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:*

*(1) Gathering and analyzing [Critical Infrastructure Information (CII)] in order to better understand security problems and interdependencies related to critical infrastructure and protected systems in order to ensure the availability, integrity, and reliability thereof;*

*(2) Communicating or sharing CII to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to critical infrastructure or protected systems; and*

*(3) Voluntarily disseminating CII to its members, Federal, State, and local governments, or to any other entities that may be of assistance in carrying out the purposes specified in this section.”*

- B. CIPC. The CIPC is one of the NERC standing committees. It is a committee that is comprised of representatives in each of the NERC Regions in the US and Canada and associations including American Public Power Association, Canadian Electricity Association, Edison Electric Institute, National Rural Electric Cooperative Association. Those representatives are subject matter experts in the areas of bulk electric system operations, physical security, and cyber security from electric utilities. CIPC provides guidance to the ES regarding strategic and tactical matters.
- C. ESCC. The ESCC is composed of the CIPC Executive Committee and a senior NERC representative. The ESCC partners with Governmental Agencies (including the Department of Energy, Department of Homeland Security, Federal Energy Regulatory Commission, Nuclear Regulatory Commission, Public Safety and Emergency Preparedness Canada) to develop security plans and enhance tactical deployment.
- D. ESISAC. The ESISAC is operated by NERC with CIPC oversight. The ESISAC has agreements regarding information sharing with the Department of Homeland Security and the other Critical Infrastructure ISACs.

### **III. Authority**

- A. *The Homeland Security Act of 2002*, 6 U.S.C. § 101 *et. seq.*, P.L. 107-296; 116 Stat. 2135 (2002).
- B. *The Homeland Security Information Sharing Act*, 6 U.S.C. § 481 *et. seq.*
- C. *The Critical Infrastructure Information Act of 2002*, 6 U.S.C. § 131 *et. seq.*
- D. *The Intelligence Reform and Terrorism Prevention Act of 2004*, PL 108-408; 118 Stat. 3638 (2004).
- E. 6 C.F.R. Part 29, *Protected Critical Infrastructure Information*

### **IV. Purpose**

This agreement defines the mutual expectations for HSIN use and support, data confidentiality, data ownership, and other matters surrounding the DHS and Electricity Sector relationship in the venture defined as the Homeland Security Information Network-Electricity Sector (“HSIN” or “HSIN-Electricity Sector”). HSIN-ES is designed to ensure that all Electricity Sector stakeholders in homeland security matters including critical infrastructure/key resource owners and operators are provided with access to internet-based communication and collaboration tools sponsored by the Department of Homeland Security. These tools, compiled into the HSIN-Electricity Sector web portal, are designed to enhance the sector’s ability to communicate, collaborate/coordinate, and maintain enhanced awareness of operationally significant situations within and concerning the sector and their commercial enterprises at no cost to the NERC or to any HSIN-ES user.

## V. Responsibilities

### A. The Electricity Sector Coordinating Council will:

1. Maintain administrative functions as the electricity sector's Sector Coordinating Council using HSIN;
2. Provide the Department with administrative points of contact for coordination with the ESCC;
3. Facilitate the registration of current and future homeland security stakeholders within the electricity sector into the HSIN-Electricity Sector user community by defining and performing registration services exclusive of governmental involvement in a manner that is fair to all stakeholders and truly representative of the electricity sector community.
4. Review and provide the Department with input, comments, and suggestions on the content and intent of the HSIN-Electricity Sector member End User Agreement;
5. Relay or provide input, comments, and suggestions to the Department of Homeland Security regarding HSIN as a communication and collaboration medium that will enhance its usefulness and value to its end users within the electricity sector;
6. Forward relevant information received from DHS or other governmental entities to electricity sector stakeholders through the relevant means of communication available to include the HSIN-Electricity Sector communication and collaboration media as appropriate;
7. Sponsor, encourage, and support to the most feasible extent possible the understanding among trade associations, owners, operators, employees, and other relevant electricity sector stakeholders that will ensure their active participation in and use of HSIN-Electricity Sector to communicate, collaborate/coordinate, and remain aware of operationally significant situations within and concerning the sector and their commercial enterprises;
8. In coordination with the Department's indication, analysis and warning program, protected critical infrastructure information program, or otherwise as appropriate; sponsor, encourage, and support to the greatest extent possible the communication of suspicious activity information and critical infrastructure information not customarily in the public domain and related to the security of Electricity Sector critical infrastructure or protected systems to Department of Homeland Security and other law enforcement and investigative interests as warranted<sup>3</sup>;
9. To exercise exclusivity of content management for products and information residing on HSIN-Electricity Sector. DHS reserves the right to conduct technical (content neutral) audits of HSIN-ES to ensure that there are no unauthorized or illegal uses of the system, and to maintain system reliability. The government cannot abrogate its

---

<sup>3</sup> Where exemption from Federal/state public disclosure under applicable freedom of information/government in the sunshine laws is desired for critical infrastructure information, all information so submitted shall be accompanied by the express statement, "***This information is voluntarily submitted to the Federal government in expectation of protection from disclosure under the provisions of the Critical Infrastructure Information Act of 2002 with the understanding that any false representations/certifications regarding this submission may constitute a violation of 18 U.S.C. 1001, punishable by fine and imprisonment.***" The submission shall also be accompanied by a signed certification stating, "***To the best of my knowledge, information, and belief, this information; 1) is voluntarily provided for the purposes of the CII Act of 2002, b) is not being submitted in lieu of independent compliance with a Federal legal requirement, 3) is not customarily in the public domain, and [as appropriate] 4) is not required to be submitted to a Federal government department or agency/4) is required to be submitted to [AGENCY NAME HERE] as required by [LEGAL AUTHORITY MANDATING SUBMISSION HERE].***"

responsibility to assure that assets it is funding are used as they are intended for the public good and are not abused. This auditing responsibility is accomplished by technical personnel whose mission is to ensure the stability and reliability of the system. They are not content managers and do not routinely take or review content.

**B. The Department of Homeland Security will:**

1. Maintain ownership, oversight, responsibility, and stewardship of the technology and functions of HSIN-Electricity Sector;
2. Subject to annual appropriations authorization and availability of legislative funding for operations consistent with this agreement, maintain stewardship of HSIN-Electricity Sector to include funding and empowering the HSIN-Electricity Sector web portal resource to:
  - i. Provide alert/warning/advisory information from and among DHS and electricity sector owners, operators, and relevant stakeholders;
  - ii. Provide the ability for electricity sector owners, operators, and stakeholders to report suspicious incidents and activities to law enforcement and the Department through one medium;
  - iii. Provide the ability for electricity sector owners, operators, and stakeholders to accomplish all of their required federal reporting obligations using HSIN-Electricity Sector (subject to the concurrence and approval of the recipient agency);
  - iv. Provide the ability for electricity sector owners, operators, and stakeholders to provide voluntary reports per the Department's Protected Critical Infrastructure Information (PCII) Program using the HSIN-Electricity Sector web portal tools;
  - v. Provide electricity Sector owners, operators, and stakeholders a document library tool with access to documents and the library restricted based upon HSIN-Electricity Sector membership and roles as defined by electricity sector. The HSIN-Electricity Sector document library would be a secure repository of information relevant to electricity sector members' business operations;
  - vi. Provide electricity sector owners, operators, and stakeholders electronic discussion spaces with access to those electronic spaces restricted based upon HSIN-Electricity Sector membership and roles as defined by electricity sector. These would allow participants, and subgroups of participants, to have secure electronic conversations with access restrictions set by the conversants.
  - vii. Conduct communication, data, and information sharing between sectors and other governmental entities.
3. Exercise best efforts in good faith to provide timely advance notice of any material change in law or regulatory policy that will or may impact the Department's ability to conduct the activities defined in paragraph 2, and elsewhere defined in this document. Such notice shall be viewed as key consideration in the relationship between the parties and essential in affording the ESCC the opportunity to explore avenues that may permit them to mirror the functionality of HSIN-Electricity Sector or to otherwise mitigate the impact of any such change in law or policy on ESCC activities.
4. Enforce and maintain the policy and operational concept for HSIN-Electricity Sector such that HSIN-Electricity Sector participant information and communications would remain their own business information unless expressly provided to the government.

This concept would respect that HSIN-Electricity Sector participants will be able to post comments or documents to portions of the HSIN-Electricity Sector website to which they have been granted access. Each member posting information to the site retains legal custody and control over that information. Such custody and control includes the exclusive authority to define who (by HSIN-Electricity Sector registration role) can have access to the information and how long the information is to remain on the site. Both ESCC and DHS would renounce responsibility for content-based control over information posted by any other entity with the caveat that DHS maintains the right to administratively audit the HSIN-Electricity Sector websites and remove any item that threatens the website's efficient operation. By policy, DHS will affirmatively hold HSIN-Electricity Sector information thus defined as to not constitute "records" subject to the Federal Records Act or "agency records" subject to the Freedom of Information Act in coordination with the Department of Justice's Office of Information & Privacy;

5. Establish and provide HSIN-Electricity Sector user names and passwords for to registrants who:
  - i. Are members of NERC/CIPC/ESCC/ESISAC,
  - ii. Are members of trade associations within the electricity sector as identified by the ESCC, and
  - iii. Are identified as owners, operators or relevant stakeholders of electricity sector critical infrastructure not otherwise members of the above but whose membership is deemed relevant to the interests of this agreement and its authorities upon coordination with or notice to ESCC;
6. Maintain a protocol for user accountability that reasonably ensures that, as HSIN-Electricity Sector users leave their relevant employment, their access to HSIN-Electricity Sector is removed; and
7. Take other actions as the Federal steward and business owner of HSIN-Electricity Sector technology and functions to integrate HSIN-Electricity Sector member individual non-consensus input into consideration in the implementation of Federal laws, policies and practices designed to promote greater information sharing between and among the federal government and private critical infrastructure.
8. Provide and maintain in coordination with the ESCC an End User's Agreement between DHS and the HSIN-Electricity Sector's registered members that defines the expectations of DHS and the ESCC for HSIN-Electricity Sector member users.

## **VI. Effective Date, Amendment, Modification & Termination**

This MOU shall become affective on the latter date of signature of the parties to the Agreement. No follow-up reports or documentation of actions taken in compliance with this MOU are required. This MOU may be modified or amended only by written mutual agreement of the parties. Either party may terminate this MOU by providing written notice to the other party.

## **VIII. Points of Contact (POCs)**

DHS Administrative POC:  
NAME  
ADDRESS  
PHONE

DHS Technical POC:  
NAME  
ADDRESS  
PHONE

EMAIL

EMAIL

NERC Administrative POC:

XXXXXX XXXX  
XXX XXXX XXXXXX  
XX XXXX XXXXXX  
XXX XXX XXXX

## **IX. Approving Officials**

On Behalf of the Department of Homeland Security

NAME / DATE  
TITLE, OFFICE

On Behalf of the Electricity Sector Coordinating Council

NAME / DATE  
BUSINESS TITLE, POSITION  
CSCC TITLE, POSITION

## **REGISTRATION EUA (HSIN-SBU/Mission Sites)**

### **Registration Notice:**

You are entering a United States Government maintained system, which may be used only for authorized information coordination conducted within HSIN-Electricity Sector to include (but not be limited to) functions such as information gathering, processing, dissemination, sharing, archiving, and the general business records management practices associated with Federal, state, municipal, tribal, and private sector information management and exchange. HSIN may not be used for lobbying, advertising, or product endorsement. Unauthorized attempts to gain access, upload, and/or change information on this web site may be a violation of Federal and/or state criminal law

### **Monitoring and Auditing:**

Use of this system is subject to monitoring/auditing the usage of this system to ensure the security of the network and to prevent use for any purpose constituting a violation of law.

### **Access to Information:**

The information within HSIN-Electricity Sector is limited to particular communities whose users are vetted through detailed registration, identity verification, and access validation protocols. Information reported or posted by a particular entity may be coordinated within/among the relevant or applicable community to which it was reported or posted by the source entity but remains subject to any limitations on use/dissemination imposed by the reporting/posting source entity and remains within the custody and exclusive control of the source entity agency for information privacy and information production/disclosure requirements imposed by law or regulatory policy. No information posted for HSIN-Electricity Sector membership may be released or distributed beyond this sector community membership absent the express approval of the source entity.

### **Use of Information:**

HSIN-Electricity Sector information is presumptively owned or licensed by individuals, companies, or organizations and protected by U.S. and foreign copyright laws. No information sourced from or displayed within HSIN-Electricity Sector shall be used in a manner that may subject individuals, companies, or organizations to commercial harm, competitive injury, or regulatory action.

**Registration Disclaimer:** This site is merely maintained by the U.S. Government who neither controls nor manages its content or access to its information. The information communicated on this system may be pre-analytical and unconfirmed information from numerous sources. The U.S. Government does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or processes disclosed through this system. The U.S. Government does not endorse or recommend any products, processes, or services of non-federal or commercial entities. The views and opinions expressed within products on HSIN-Electricity Sector do not state nor reflect those of the U.S. Government. HSIN-Electricity Sector web pages may provide links to external internet sites for the convenience of its users but the U.S. Government is not responsible for the availability or content of those external sites and does not endorse, warrant, or guarantee the products, services, or information described or offered at those other internet sites. The compliance policies and rules concerning information coordination required for access to HSIN-Electricity Sector are not intended to create or confer any right, privilege, or benefit to any private person including any person in litigation with the United States or any agency or individual using HSIN.