

## North American Electric Reliability Council

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

### CRITICAL INFRASTRUCTURE ADVISORY GROUP (CIPAG)

#### Agenda

Draft-2

#### Meeting Schedule

The Critical Infrastructure Protection Advisory Group meets:  
Thursday (0800-1700 hr) – Friday (0800-1500 hr), 01-02 May 2003  
Attire is casual.

Meeting Location	Sleeping Rooms
Buena Vista Hotel 8203 World Center Dr. Orlando, FL 32821 tel: 407-239-8588	(adjacent hotel) Caribe Royale All Suites Resort Orlando, FL tel: 407-238-8000

#### Attachments

1. Minutes of the NERC CIPAG Meeting 16-17 January 2003, draft-1
2. Minutes of the NERC CIPAG Meeting 07-08 November 2002, final
3. CIPAG Roster, Members, Alternates, 23 April 2003
4. CIPAG Scope
5. CIP Task Force Scopes and Rosters
6. Electricity Sector Critical Infrastructure Protection Communications, 18 April 2003.
7. CIP Workshops for the Electricity Sector
8. Security Guideline: Securing Remote Access to Electronic Control and Protection Systems, version: 0.3.1
9. Security Guideline: Threat and Incident Reporting, version: 0.9
10. DHS Procedures for Handling Critical Infrastructure Information; Proposed Rule, 15 April 2003

#### Agenda

1. Meeting logistics:
  - a. NERC anti-trust compliance guidelines.
  - b. Introductions of the CIPAG members, alternates, associates.
  - c. Review the new CIPAG scope, now in place.
  - d. Review NERC committee procedures.
  - e. Plan any task force breakout activities.
    - i. ESISAC, Communications
    - ii. Cyber Security Standard
    - iii. Security Guidelines
    - iv. Other.
  - f. **(Action)** Amend and approve this agenda.
2. **(Action)** Amend and approve minutes of the 16-17 January 2003 meeting.
3. Future meetings, conference calls, and presentations:
  - a. CIPAG: Thursday-Friday, 17-18 July 2003 with NERC Standing Committees in Albuquerque, NM.
  - b. Next.
  - c. Conference calls as required.
4. Presentation on EMP and action plan to address issues raised. Jim Silk, IDA.

5. Vulnerability of Extra-High-Voltage (EHV) Electrical Transformers of the CONUS Power System to Terrorist Attack, Ted Heller (Thursday).
6. Cyber Security Standard and urgent action status, Chuck Noble.
7. Process Control Systems Security Task Force report, Scott Mix.
  - a. **(Action)** Approve for presentation to the NERC Board: Security Guideline: Securing Remote Access to Electronic Control and Protection Systems, version: 0.3.1.
8. **(Action)** Approve for presentation to the NERC Board: Security Guideline: Threat and Incident Reporting, version: 0.9, Stuart Brindley.
9. Electricity Security Guidelines application survey.
10. Public Key Infrastructure Project report, Larry Bugh.
11. Cyber Log Analysis Initiative report, Stuart Brindley.
12. DHS report. Nancy Wong (Friday).
13. DHS-IAIP report. Michael Cohen.
  - a. Consider modifications to the Indications, Analysis, Warnings Program procedure.
14. ESISAC report.
  - a. Expected and improved communications.
  - b. Discussions with other ISACs.
  - c. Proposed exercise. John Maguire.
  - d. Automated Critical Incident Event Reporter, Scott Mix.
  - e. Department of Homeland Security Procedures for Handling Critical Infrastructure Information, proposed rule.
15. Report on CIP Workshops.
16. Critical Spares Project, Mike Innocenzo, Gerry Cauley.
  - a. Protocol for use of the database.
17. Impact of SQL Slammer.
18. DOE report. Craig Zingman.
  - a. Status of the Federal Emergency Response Plan.
19. NERC report.
20. Organization and Agency reports as available:
  - a. APPA.
  - b. CEA.
  - c. EEI.
  - d. EPRI.
  - e. FERC.
  - f. JPO.
  - g. NAESB.
  - h. NRC.
  - i. NRECA.
  - j. NSA.
  - k. OCIPEP.
  - l. RUS.
  - m. USSS.
  - n. Other.
21. Feedback from meetings and conferences attended by members.
22. **(Action)** Review CIP Task Forces.
23. Cyber experience learnings. Herman Green.
24. Roundtable discussion:
 

All CIPAG participants are encouraged to share including recent events, incidents, and policy (pens down as requested by presenters):

  - a. Physical incidents
  - b. Cyber incidents.
25. Other.

These minutes are for the use of the NERC Critical Infrastructure Protection Advisory Group and the ES-ISAC as the participants of these bodies deem appropriate. These minutes are not for public distribution.

**NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL  
CRITICAL INFRASTRUCTURE PROTECTION ADVISORY GROUP  
MEETING MINUTES  
16-17 JANUARY 2003; PHOENIX, AZ**

**DRAFT-1**

CIPAG information on the Internet: <<http://www.nerc.com>> (Download files: Critical Infrastructure Protection); <<http://www.esisac.com>>

This meeting was announced in the minutes of the 07-08 November 2002 CIPWG meeting and in email dated 05 November 2002. The NERC Anti-trust Guidelines were read. A quorum was established.

**Attendees**

Kevin Perry, Chair	SPP	Ken Hall	EEI
Larry Bugh, V Chair	ECAR	Brian Hogue	NPCC
Mike Lynch, V Chair	Detroit Edison	Scott McCoy	Xcel Energy
Bob Windus	BPA	Eric Solberg	ATC
Stuart Brindley	CEA	Wally Johnson	PEPCO
Gene Byars	SOCO	Roger Lampila	NYISO
Jerry Freese	AEP	Bonnie Bushnell	NYISO
Herman Green	Alliant En	Pat Laird	Exelon
Chuck Noble	ISO-NE	Larry Brown, c/c	EEI
Tom Flowers	CenterPoint	Mike Hagee	Duke Energy
Floyd Galvan	Entergy	David Thomason	Reliant En
Lyman Shaffer	PGE	Bob Canada	SOCO
Bob Sypult	SCE	John Fridye	Reliant Resources
Barry Lawson	NRECA	Patrick Lee	SDG&E
Marc Nichols	OPPD	Scott Heffentrager	PJM
Mike Zahorik	ATC	Tim Deloach	Sempra En
Abbie Layne	DOE, NETL	Jim Davis	Ontario Pow Gen
Ted Heller	JPO	Robert Bass	PNNL
Ron Smith	CIAO, USSS	Michael Cohen, c/c	NIPC
Tom Phinney	Honeywell Labs	Joe Graziano	Alstom
Joe Weiss	KEMA	Mike Beehler	Burns & McD
Jim Fortune	EPRI	Scott Mix	EPRI
George Miserendino	Tritonsec	Bill Flynt	TRC
Bob Cummings, c/c	NERC	Lou Leffler	NERC

c/c: Participated via conference call on some or all of the following topics:

1. Reports from NIPC, NRC, CIAO
2. Critical Spares Initiative.

**Acronyms**

AtA	Approach to Action	ICCP	Inter-control Center Communications Protocol
-----	--------------------	------	--

CIP	Critical Infrastructure Protection	IDS	Intrusion Detection System
CIPAG	Critical Infrastructure Protection Advisory Group	ISCG	Information Sharing and Coordination Group
CIPIS	Critical Infrastructure Protection Information System	NERC	North American Electric Reliability Council
DHS	Department of Homeland Security	NIPC	National Infrastructure Protection Center
DOE	Department of Energy	OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness
ES	Electricity Sector	OHS	Office of Homeland Security
ES-ISAC	Electricity Sector-Information Sharing and Analysis Center	PCS	Process Control System
FERC	Federal Energy Regulatory Commission	PKI	Public Key Infrastructure
IAIP	Information Analysis – Infrastructure Protection	SAR	Standard Authorization Request
IAW	Indications, Analysis, and Warnings	SDWT	Self Directed Work Team

### Next Meetings

1. CIPAG: Thursday (0800-1700 hr)-Friday (0800-1500 hr), 01-02 May 2003; Orlando, FL

### Conference Calls

To be arranged for the CIPAG and SDWTs as required.

### Documents

1. CIPAG Roster
2. CIPAG SDWT Rosters

### Action Items

1. Forward the proposed Security Guide: Securing Remote Access to Electronic Control and Protection Systems to the IEEE.
2. Lou Leffler will pursue status of requested clearances through the DOE.
3. A cleared briefing in DC will be requested.
4. A set of CIP related definitions and a taxonomy will be developed.
5. Follow up with library of resources from the USSS.

### Topics for Future Meetings

1. CIP coordination between NERC and NAESB.
2. Consider evaluating the impact on the ES of inability to use the Internet.

### Distributions

1. IDS Log Analysis, Stuart Brindley
2. DOE Energy Infrastructure Assurance Technology Roadmap, Abbie Layne
3. Incident Command System (ICS), Herman Green
4. Overview of the USSS Electronic Crimes Branch, Ron Smith
5. Spare Equipment Project, Bob Cummings
6. ES-ISAC presentation, Lou Leffler

### Motions

**Motion 1:** Moved: Gene Byars; Seconded; Action: Passed, no dissenting votes.  
Approve agenda for this meeting.

**Motion 2:** Moved: Larry Bugh; Seconded; Action: Passed, no dissenting votes.  
Approve minutes of the 06-07 November 2002 meeting, draft-1.

**Motion 3:** Moved: Gene Byars; Seconded; Action: Passed, no dissenting votes.  
CIPAG endorses language regarding the CIPAG in the "Review of the Future Role of NERC Committees", draft-8 as recommendation-4 in the Executive Summary (language copied below under CIPAG Organization).

**Motion 4:** Moved: Gene Byars; Seconded; Action: Passed, no dissenting votes.  
Recommend to the NERC Standing Committee Executive Committee that the CIPAG have formal representation on the proposed Technical Committee.

**Motion 5:** Moved: Process Controls Security SDWT; Action: To be voted via email by close of business 24 January 2003.  
Approve the proposed Security Guide: Securing Remote Access to Electronic Control and Protection Systems (draft-16 January 2003) for forwarding to the NERC Standing Committees and public posting for comment.

**Motion 6:** Moved: Tom Flowers; Seconded; Action: Passed, no dissenting votes.  
Forward the proposed (until approved by the NERC Board) Security Guide: Securing Remote Access to Electronic Control and Protection Systems to the IEEE.

**Motion 7:** Moved: Gene Byars; Seconded; Action: Passed, no dissenting votes.  
Add North American Energy Standards Board (NAESB) to item-3 under Activities in the proposed CIPAG Scope.

**Motion 8:** Moved: Gene Byars; Seconded; Action: Passed, no dissenting votes.  
CIPAG accepts the revised CIPAG Scope for submittal to the NERC Board.

**Motion 9:** Moved: Michael Lynch; Seconded; Action: Passed, no dissenting votes.  
CIPAG accepts the revised Organization Transition Plan for submittal to the NERC Board.

### **General**

Herman Green was thanked for all his efforts to help secure the ES in the development of National Plans input and the CIP Workshops, among other significant contributions.

### **CIPAG Organization**

The proposed revised CIPAG Scope and a transition plan will be sent to, and discussed with, the NERC Board of Trustees at the Board's February 2003 meeting.

Michael Lynch, Kevin Perry, and Larry Bugh attended two meetings with the NERC Standing Committees Executive Committee (SCEC) on behalf of the CIPAG to support the continued reporting relationship of CIPAG directly to the Board. The SCEC supports this continued relationship for at least one year with review. The SCEC strongly recommended (and CIPAG agrees) that significantly more communication must be established between CIPAG and the Operating, Planning, and Market Interface Committees (the Standing Committees) and from CIPAG members to their Regions and Associations.

Distribution of the full CIPAG minutes is restricted due to security concerns. Minute highlights will be prepared for each CIPAG meeting (starting with the January 2003 meeting) that can be distributed in the usual NERC manner which is open. The formal CIPAG minutes (with attachments) will be shared with the SCEC and the new, proposed NERC Technical Committee. CIPAG cautioned about excessive "sanitization" of the minutes; care will be exercised.

The following language (from "Review of the Future Role of NERC Committees", draft-8) will be included in the CIPAG Scope:

"On an interim basis, retain the Critical Infrastructure Protection Advisory Group (CIPAG) as an advisory group reporting to the Board. Periodically review the CIPAG scope and organization, with a preference in the future toward integrating the critical infrastructure protection function into the technical committee(s)."

### **CIPAG Organization Transition Plan**

The transition plan was reviewed. The revised membership will include three representatives from each NERC Region (one each with the following expertises: Physical Security, Cyber Security, Operations; with consideration to skills in Policy matters), and two representatives from the Associations (APPA, CEA, NRECA), with consideration to the skill sets. Alternates from each Association and Region are strongly encouraged. Descriptions of the disciplines will be written and disseminated. NERC Regional Managers are points of contact; their contact information is in the NERC Roster (Regional Manager section) (the Roster is posted at the NERC Internet site).

The transition is expected to be complete for seating new members at the May 2003 CIPAG meeting (next meeting).

### **CIPAG Meeting Frequency**

There was discussion on how often the CIPAG should meet as a general rule, recognizing the need for extra meetings under certain circumstances. Self Directed Work Teams will meet as required to complete their taskings.

As stated in the proposed revised CIPAG Scope: CIPAG meetings will be conducted at the discretion of the Chair, generally on a quarterly basis. Following are comments:

1. Concern for insufficient number of meetings.
2. Concern for travel.
3. Possibly conduct four meetings in addition to those conducted during the EEI Security Committee meeting weeks.
4. Great concern for getting SDWT work done and approved.
5. Consider synchronizing with the timing of the Board meetings.
6. Consider more use of conference calls and use of Internet meeting technology.
7. Try for four meetings with more if required.
8. Consider a central meeting place.
9. Possibly conduct four business meeting each year with workshops focussed on specific topics.

### **Process Control Systems Security (PCSS)**

Scott Mix described the proposed Security Guideline: Securing Remote Access to Electronic Control and Protection Systems (draft-16 January 2003). The CIPAG agreed (Motion-5) to an email ballot to approve posting this Security Guideline for comment.

### **Security Guideline: Threat and Incident Reporting**

The proposed Security Guideline: Threat and Incident Reporting (version-0.8) was presented by Stuart Brindley. CIPAG members made suggestions for changes to include reference to the DOE Form-417 reporting and clarifications to proprietary treatment.

(Subsequent to this meeting the CIPAG approved posting the revised proposed Security Guideline for industry comment. The approved – by email – Motion: Accept Security Guide: Threat and Incident Reporting, draft 0.9, for industry comment posting.)

It is agreed that there must be further consideration to tying Form-417 reporting to Threat and Incident Reporting in an appropriate and proprietary manner including reporting mechanics. Personnel currently are required to make duplicate reports, and this can be time consuming under stressed conditions.

#### **Critical Spares Initiative (Via conference call)**

Bob Cummings provided an update on the initiative. The presentation is included in the minutes distributions. Access to the spares database, which is nearly complete, can be registered.

#### **Public Key Infrastructure Project (PKI)**

Larry Bugh reported on the implementation of PKI as approved by the Board. The following organizations are currently working together to establish PKI for the Energy Sectors: NERC, NAESB, AGA, API.

Specific details include:

1. PKI architecture will include:
  - A. Certificate encryption and/or digital signature.
  - B. Certificate validation.
  - C. Key backup.
2. There will be a hierarchy of Certificate Authorities (CA). One will be the root CA.
3. There will be a registration process to obtain (assure affiliation and need for a certificate) and revoke certificates. It is envisioned that for the ES there will be a Registration Authority on a Regional basis.
4. Certificated sessions will time out after 12 hours.

#### **Cyber Log Analysis Project**

Stuart Brindley reported on the work done by one organization using tools of one vendor. The importance of documenting and analyzing attempted intrusions is highlighted by the significant increase of attempts to intrude into systems. Results include worm vs non-worm analysis, most popular ports attacked, number of incidents/week, top ten source countries (though not necessarily the real source).

Recommendations:

1. Tune the rules to the environment.
2. Log full alarm packets.
3. Consider logging additional data.
4. Dedicate resources to IDS support and data analysis.
5. Implement incident handling and response policies/procedures.
6. Deploy a consistent set of tools and techniques.

Conclusions:

1. The IDS analytical means exist.
2. Need agreement to share data.

Stuart will develop a business case for CIPAG review:

1. Scope.
2. Business benefits.
3. NIPC and intelligence benefits.
4. Data confidentiality.
5. Cross border issues and opportunities.
6. Cross sectoral opportunities (eg financial institutions).

IDS log analysis can lead to early warning of an attack on a Sector and/or National basis. We will seek funding from Governments (estimated funding per participant for a year in real time: \$100,000 max). Board approval will be requested.

### **Critical Infrastructure Assurance Office (CIAO)**

Ron Smith reported that Nancy Wong is Acting Director of the CIAO. She will lead the effort to transition to the Department of Homeland Security (DHS). NIPC and Office of Energy Assurance will also transition to DHS in the Information Analysis – Infrastructure Protection (IAIP) section, and the personnel will merge as this will be a single, unified organization.

The CIP Business Cases for Action are not completed. It is necessary to determine the need for these and develop a plan for their completion.

### **DOE Technology Roadmap**

Abbie Layne updated the CIPAG on the DOE's Energy Infrastructure Assurance Technology Roadmap. The presentation is included in the minutes distributions. This work will transition to the DHS. Other related efforts include: National Infrastructure Simulation and Analysis Center (NISAC), Training Center, SCADA test beds.

An R&D Steering Committee for the Energy Sectors will be established. This will be executive level with subject matter support with an objective to assure direction in prioritizing development of the physical and cyber R&D Roadmap. The functional areas included are: prevention, detection, mitigation, reconstitution. Physical and cyber interdependencies will be treated. An R&D whitepaper will be reviewed by the Steering Committee. This work will be treated initially as sensitive, some may be classified.

There will be three industry workshops in the March – April 2003 timeframe: Electricity Generation and Delivery, Pipeline Delivery, Fuel Processing and Storage.

There is a proposed development of training for plant operators to assist them in recognizing unusual "behaviors".

### **Update on NAESB and SAR Process**

Wally Johnson provided an update on the development of the NERC – North American Energy Standards Board (NAESB) relationship and the Standards Authorization Request process.

Existing NERC Policy is not metric oriented. The ANSI approved process will provide measurable, enforceable standards. CIP guidelines can be considered for standards.

The impact of the Market on Operations and vice versa are treated in the NERC-NAESB memorandum of understanding. The relationship will determine what practices, processes, policies require standards development. The Joint Interface Committee (JIC) will determine standards requirements. It will be requisite to coordinate CIP between NERC and NAESB.

### **Electric Power Research Institute (EPRI)**

Jim Fortune reported that EPRI has developed a physical/cyber risk assessment methodology in report format, with a CD including the forms used in the method. The method treats assessing critical assets with a view to defining criticality. The R-B-G approach is used in matrix form to help assess the types of attacks that may be pertinent for inclusion in planning. The ES Security Guidelines and FERC Standards are referenced. How to do penetration testing is presented. Access to the report is expected to be from EPRI at nominal cost. The Enterprise Information Security (EIS) group did the development.

### **Incident Command System**

Herman Green presented concepts for the implementation of an Incident Command System (ICS); the presentation is included in the minutes distributions.

Some attendees reflected on use of an ICS as being difficult to adapt in an electricity organization. Others believe there is need for the concept if not all the detail implementation. It also provides for a known set of personnel to deal with an emergency and to keep it as seamless as possible with normal operations.

### **National Infrastructure Protection Center (NIPC)**

Michael Cohen reported that, effective 01 March 2003, the current NIPC activities will move to the Department of Homeland Security under the IAIP Division. Details of personnel are not available. Basic functions include threat, vulnerability mapping, remediation of vulnerabilities and reduction of risk, competitive analysis ("red teaming"), and others.

### **Nuclear Regulatory Commission (NRC)**

Al Tardiff and Bob Bass reported that a cyber assessment project for reactors has been established. Orders and later Code of Federal Regulations (CFR) may be issued in this area. Specific measures are expected for each site.

A revised nuclear facility design basis threat is expected in the March 2003 timeframe.

Licensees will have assessment methods to examine vulnerabilities of digital assets used to control nuclear plant. The intent is to cover all systems to determine common vulnerabilities. Plant operations can also be examined. The generic methodology is expected to be complete by mid-2003. The methodology will be discussed with the nuclear industry.

### **US Secret Service (USSS)**

Ron Smith discussed the proposed partnering between the USSS, the ES, and the ES-ISAC. The USSS is a resource to the ES. A library of reference materials will be made available.

### **Electricity/Telecommunications Interdependency Assessment,**

Stuart Brindley reported on this interdependency considering the critical dependence of the ES on Telecommunications. There is much mutual interdependency between these sectors. The question is how to deal with this on a scenario basis? Stuart reported on work being done in one organization.

There are defined priority telecommunications paths related to ES facilities and operations. There are technical requirements for normal and high priority telecommunications paths; eg: provision to withstand loss of power for at least eight hours, physically diverse paths (routing).

Some organizations are phasing out reliance on legacy microwave due to expansion difficulties and lower cost alternatives. This leaves Public Switched Telephone Network (PSTN) and satellite.

This work has led to partnering between ES and Telcom to determine critical ES locations. Telcom then identifies the substantial security nature of the telcom facilities serving the critical ES locations.

Judgement is that a widespread telcom failure scenario due to natural causes is not credible. Local telecom failure can be mitigated by use of MSATs (Mobile SATellite). MSAT is used for voice.

Cross-sector coordination is being established including communication protocol between ES, Telecom, Banking and finance.

The CIPAG was requested to indicate individual interest in working on an exercise to determine definitively the impact on the ES due to loss of Telcom. There is a meeting proposed with the National Communications Commission sometime this winter.

### **Reliability Assessment Methodology (RAM) Products,**

Bob Windus provided an update on the RAM products. RAM-D (Dams) has been used to evaluate several facilities. The result was a clear picture of the risk in a standardized matrix. The process requires in depth analysis of the impact of an attack.

Using RAM-T (Transmission) has been used to evaluate many stations. This analysis is leading to a baseline security program. Likelihood of attack, consequence of attack, security in place are the three factors that lead to risk management. Results of the RAM analyses have led to many security actions being approved.

Physical steps include more and improved fencing, more monitoring, and remote access to the monitoring.

Sandia National Laboratory is in the process of establishing a school for training in the products. Software products will soon be available. Bob Windus will provide the contact.

Now available: RAM-D (Dams), RAM-T (Transmission), RAM-W (Waterworks); and in the works, RAM-F (Fossil).

### **Roundtable**

A pens down roundtable was conducted.

These minutes are for the use of the NERC Critical Infrastructure Protection Advisory Group and the ES-ISAC as the participants of these bodies deem appropriate. These minutes are not for public distribution.

**NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL  
 CRITICAL INFRASTRUCTURE PROTECTION ADVISORY GROUP  
 MEETING MINUTES  
 07-08 NOVEMBER 2002; TAMPA, FL**

**FINAL**

CIPAG information on the Internet: <<http://www.nerc.com>> (Download files: Critical Infrastructure Protection); <<http://www.esisac.com>>

This meeting was announced in the minutes of the 26-27 September 2002 CIPWG meeting and in email dated 30 September 2002. The NERC Anti-trust Guidelines were read. A quorum was established.

**Attendees**

Kevin Perry, Chair	SPP	Ken Hall	EEl
Larry Bugh, V Chair	ECAR	Brian Hogue	NPCC
Mike Lynch, V Chair	Detroit Edison	Mike Hyland	APPA
Jack Bernhardsen	PNWSC	Len Januzik	MAIN
Stuart Brindley	CEA	Wally Johnson	PEPCO
Gene Byars	SOCO	Roger Lampila	NYISO
Paul Cafone	PSEG	Brian Malfant	FRCC
Linda Campbell	FRCC	Paul McClay	Tampa El
Franklin Dessuit	NiSource	Scott McCoy	Xcel Energy
Tom Flowers	CenterPoint	Scott Mix	PJM
Floyd Galvan	Entergy	Brad Morrow	Tampa El
Joe Gracia	TVA	Eric Solberg	ATC
Mike Hagee	Duke Energy	Terry Luddy, c/c	Duke
Larry Brown, c/c	EEl	Chuck Noble, c/c	ISO-NE
Phil Donegan, c/c	Pacificorp	Bob Sypult, c/c	SGE
Pat Laird, c/c	Exelon	Glenn Coplton	NIPC
Bill Flynt	DOD	Ted Heller	JPO
Alison Silverstein, c/c	FERC	Ron Smith	CIAO, USSS
Thomas Kropp	EPRI	Mike Beehler	Burns & McD
Tom Boudewyns	OATI	Catherine Cook	Alstom
Joe Weiss	KEMA	Bob Cummings, c/c	NERC
Lyn Costantini	NERC	Ron Niebo	NERC
Lou Leffler	NERC		

c/c: Participated via conference call on some or all of the following topics:

1. FERC NOPR on SMD Security Standards.
2. CIPAG Organization.
3. FERC NOPR on Critical Energy Infrastructure Information.
4. Critical Spares Initiative.

**Acronyms**

AtA	Approach to Action	ISCG	Information Sharing and Coordination Group
CIP	Critical Infrastructure Protection	NERC	North American Electric Reliability Council

CIPAG	Critical Infrastructure Protection Advisory Group	NIPC	National Infrastructure Protection Center
CIPIS	Critical Infrastructure Protection Information System	NS	National Strategy
DOE	Department of Energy	OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness
ES	Electricity Sector	OHS	Office of Homeland Security
ES-ISAC	Electricity Sector-Information Sharing and Analysis Center	PCS	Process Control System
FERC	Federal Energy Regulatory Commission	PKI	Public Key Infrastructure
IAW	Indications, Analysis, and Warnings	SAR	Standard Authorization Request
ICCP	Inter-control Center Communications Protocol	SDWT	Self Directed Work Team

### Next Meetings

1. PCSS SDWT: Wednesday (0800-1700 hr) 15 January 2003; Phoenix, AZ
2. CIPAG: Thursday (0800-1700 hr)-Friday (0800-1500 hr), 16-17 January 2003; Phoenix, AZ

### Conference Calls

To be arranged for the CIPAG and SDWTs as required.

### Documents

1. CIPAG Roster
2. CIPAG SDWT Rosters

### Action Items

1. CIPAG Organization SDWT to develop a transition plan.
2. Lou Leffler will pursue status of requested clearances through the DOE.
3. A cleared briefing in DC will be requested.
4. A set of CIP related definitions and a taxonomy will be developed.

### Topics for Future Meetings

1. SAR process for security standards.
2. Security Guideline: Process Control Systems Security: Remote Access.
3. Comments on the DOE document, "21 Steps to Secure SCADA.
4. Cyber log analysis project.

### Distributions

1. Refer to agenda package.
2. CIPAG Scope, draft: 08 November 2002.
3. Security Guide: Process Control Systems Security: Remote Access, draft version 0.1.
4. Critical Energy Infrastructure Information response presentation, 07/08 November 2002.
5. Update on the Electricity Industry's Spare Equipment Initiative, 08 November 2002.
6. Generic Sniper Response, 06 November 2002.
7. CIP Workshops, draft-7.

### Motions

**Motion 1:** Moved: Michael Lynch; Seconded; Action: Passed, no dissenting votes.  
Approve agenda for this meeting.

**Motion 2:** Moved: Michael Lynch; Seconded; Action: Passed, no dissenting votes.  
Approve minutes of the 26-27 September 2002 meeting, draft-2.

**Motion 3:** Moved: Stuart Brindley; Seconded; Action: Passed, no dissenting votes.

The Process Control System Security Self Directed Work Team shall continue development of the Security Guideline: Process Control Systems Security: Remote Access for subsequent approval by the CIPAG and NERC Board.

**Motion 4:** Moved: Roger Lampila; Seconded; Action: Passed, no dissenting votes.

The comments to the NERC responses to the FERC NOPR on Standard Market Design regarding Security Standards discussed and agreed to at this meeting will be incorporated.

**Motion 5:** Moved: Eric Solberg; Seconded; Action: Passed, no dissenting votes.

Accept the CIP Workshop cities as shown in workshop plan, draft-7.

**Motion 6:** Moved: Linda Campbell; Seconded; Action: Passed, 12 yes, 2 no.

The CIPAG accepts the CIPAG Scope, draft dated 07 November 2002. {Noted that additional work on the Governance section would be completed on 08 November 2002.}

**Amendment to Motion 6:** Moved: Kevin Perry, Seconded, Action: Failed.

{For Voting Members:} One representative from each Region, one from each Segment {using the NERC Planning Committee model}, and at large representatives to complete a voting roster with discipline balance among physical security and cyber security, with a total not to exceed 30.

**Motion 7:** Moved: Tom Flowers, Seconded; Action: Passed, no dissenting votes.

The CIPAG accepts changes to the CIPAG Scope, Governance section: newest Scope draft dated 08 November 2002.

**Amendment to Motion 7:** Moved: Scott Mix; Seconded; Action: Passed, no dissenting votes.

Add in Governance Section of the CIPAG Scope that only Roster Alternates may be designated proxies.

**Motion 8:** Moved: Scott Mix, Seconded; Action: Passed, no dissenting votes.

The CIPAG accepts the Critical Energy Infrastructure Information response for submittal to the FERC by 15 November 2002.

**Amendment to Motion 8:** Moved: Mike Hyland, Seconded; Action: Failed, 5 yes, 7 no.

Change Recommendation-4 on response time from 30 to 15 days.

**Motion 9:** Moved: Ken Hall; Seconded; Action: Passed, 12 yes, 1 no (Brian Malfant).

The CIPAG endorses the following recommendations to the Board for further technical and funding development with an initial funding requirement not to exceed \$100,000 for expansion of the Spare Equipment Database.

1. Expansion of NERC Spare Transformer database, phase-2 with protocols for use.
2. Enhance existing equipment sharing and other activities to support recovery from an "isolated" attack.
3. Develop and implement an industry recovery strategy based on a "scattered" attack.
  - A. Quickly task NERC to move forward on a more in-depth analysis and implementation.
  - B. Proceed immediately to develop:
    - a. Governance and administration
    - b. Equipment sharing protocols
    - c. Funding.

The CIPAG noted with sorrow the death of Linda Franklin, NIPC, who had worked with the CIPAG during development of the NERC-NIPC IAW Program.

## General

Update on NERC including the Board meeting in October 2002, the upcoming Standing Committees meetings, the relationship between NERC and NAESB.

Wally Johnson briefed on actions taken by DC area utilities in response to the sniper.

Meetings were held recently by the ES-ISAC and representatives of the DOE and JPO related to system data in support of various missions. This is explorative to determine kinds of data, availability, and usefulness. Appropriate approvals will be needed before proceeding to data submission.

### **Security Standards in the FERC Standard Market Design (Open via conference call)**

Refer to Motion: 4.

Comments discussed by the CIPAG will be incorporated. NERC will file with the FERC the CIPAG's comments on the Security Standards contained in the SMD NOPR.

The FERC technical conference on the Security Standards will be held in at the FERC offices in DC on Friday 06 December 2002. Representatives of other security related groups will be in attendance. Chuck Noble and Kevin Perry will represent CIPAG; other CIPAG members are encouraged to attend. This is an open meeting.

The dates included in the proposed FERC Standards (substantial compliance by January 2004, complete compliance by January 2005) appear reasonable, assuming a ruling is made in early 2003. There will be more known following the FERC Technical Conference, 06 December 2002. Linda Campbell suggested injecting the Security Standards into the NERC Standards process, particularly if it appears there may be delays at the FERC. Wally Johnson and Larry Bugh cautioned that initiation of the SAR process before FERC action may be premature (recognizing that the final rule may be substantially different from the NERC proposal).

The SAR process requires that Standards written to support the NERC reliability model definition must be measurable so as to be enforceable (after enforceability becomes a NERC function). Also, noted that there may be some dual responsibility between NERC and NAESB in the development of the subject Security Standards. There appears to be no reason to proceed with a SAR on the FERC Security Standards until FERC action is known. This is the consensus of the CIPAG.

There are other Standards to be developed using the SAR process; consider the existing Security Guidelines. A SAR process will be considered to cover the NERC-NIPC Indications, Analysis, Warning Program.

### **Process Control Systems Security (PCSS)**

Refer to Motion: 3.

Scott Mix, Chair, discussed the work of the PCSS SDWT that met for the second time on 05 November 2002. The SDWT has drafted a first (of what may be five or six in total) Security Guideline for PCSS. The draft is titled: Process Control Systems Security: Remote Access, version 0.1. The SDWT seeks comment on the guideline from CIPAG members. Comments will be considered in creating a version 0.2 that will be presented to the CIPAG at the January 2003 meeting for approval to request NERC Board approval at its February 2003 meeting.

The DOE document, "21 Steps to Secure SCADA", has been available for about a month. Joe Weiss has commented on the document; these were shared with the PCSS SDWT. Comments can be submitted to the DOE by the CIPAG. A draft set of comments will be prepared by Scott Mix (Chair), Joe Weiss, Frank Dessuit, Kevin Perry.

### **CIPAG Organization (Open via conference call)**

Refer to Motions: 6 and 7 and Amendments to Motions: 6 and 7.

The discussion on organization was conducted during most of the afternoon on 07 November 2002 with some carryover to 08 November 2002.

The CIPAG Scope dated 04 November 2002 was modified and approved by the CIPAG as draft dated 08 November 2002. Modifications:

1. Activities were changed to be substantially coincident with wording in the document approved by the CIPAG at the June 2002 meeting.
2. Added under "Voting Members":  
If other entities, not represented in this model, request such representation, this will be considered through the Executive Committee for CIPAG approval at the next CIPAG meeting, subject to NERC Board veto.
3. Removed from "Voting Members":  
No single organization will have more than one regular voting member. (Due to vagueness of the word organization.)
4. Under "Governance" the definition of proxy was changed to permit designated proxies from among roster alternatives to help assure a cognizant voting body.
5. Under "Governance" the meeting periodicity was modified to be a little less prescriptive.

Following are discussion points:

1. Let people vote if they attend with regularity.
2. May be difficult to obtain all the people on the proposed roster chart.
3. How collaborate with the EEI Security Committee? Concern for future disconnect. Suggestion: meet together periodically. Asset owner representatives will be to some extent from EEI companies. Working with EEI Security Committee best done by coordination through leadership and mutual working together on issues.
4. Concern for too many members. Reconsider with a view toward the NERC segment model.
5. Need operations to tie security (physical and cyber) into the overall NERC reliability intent. Need to marry physical and cyber initiatives.
6. Need to assure technical nature of CIPAG work remains the group's focus.
7. Concern for number of people.
8. Maintain contacts with other groups, eg: Operating Committee.
9. Two needs: technical activities, communications.
10. As Standing Committees get organized, the CIPAG could fit in {to those models}.
11. The CIPAG's work is critical to the security of our nations.
12. Concern for reporting directly to the NERC Board.
13. May need scope/mission review. Others believe we are beyond that now – for now.
14. CIPAG seen as a group of people with considerable expertise.
15. Regional representation also requisite to support getting information back to the user organizations.
16. CIPAG has been an esoteric group. Concern for loss of "character" by being overly rigid.
17. SDWTs can be populated by expertise whether on CIPAG formally or not. This has worked effectively.
18. Folks at CIPAG meeting want to be here. This is tribute to the group. Concern for loss of this passion and functioning cohesiveness if the CIPAG becomes too prescriptive.
19. Another model: weighted by discipline and one vote each discipline was suggested.
20. If there are specific problems, solve those.
21. Perhaps just extend voting privilege to those who attend, with one vote per particular entity.
22. Don't let voting foil the effort – it's too important.
23. Concern for being able to establish meeting quorums.
24. Concern there may possibly be need for more than four meetings per year.
25. With four meetings per year, voters will more likely attend. Much actual work is done in SDWTs.
26. Recruit for SDWTs more broadly from the ES.
27. The CIPAG had a problem with insufficient Physical Security representation. This is being resolved. A concern was raised for possible loss of the excellent expertise currently embodied in the CIPAG membership.

28. Will Distribution be covered by CIPAG? Perhaps not a part of the traditional NERC focus (bulk systems), but certainly Distribution will be covered as part of CIPAG focus and ES-ISAC operations.
29. It is likely that the other NERC Standing Committees will have different voting organizations from each other.
30. Not comfortable that this voting model truly meets the NERC objective: Fair, Open, Balanced, Inclusive.
31. Not sure that the change in CIPAG voting membership is needed. What's broken? Will the change make CIPAG more effective?
32. One representative on the Organization Team strongly supported the original recommendation.
33. It was noted that many of these concerns were considered by the CIPAG Organization Team. This Team worked very diligently to develop the draft Scope over the past month via several conference calls and one meeting.

### **Critical Energy Infrastructure Information (CEII)** (Open via conference call)

Refer to Motion: 8 and Amendment to Motion: 8.

Ron Niebo presented the work of the Team that drafted a response to the FERC NOPR on CEII. Refer to the presentation and the filing materials.

There was CIPAG discussion on the section in the response stating:

“...submitter be given at least 30 days to respond to a Commission determination that CEII will be released to a non-governmental requestor. {Currently “at least five days” stated in Part 388.112 (d).}”

Concern for not having needed information in a sufficiently timely manner to make needed decisions that argues for reducing from 30 days or indeed keeping five days. The counter argument is that it takes time to consider release of information and establish an appropriate response.

The 30 days was retained; refer to Amendment to Motion-8.

Comments:

1. Over time the currently, now available, information becomes old; there is a shelf life, an entropic life.
2. Make the obtaining of new, sensitive information harder. Force a terrorist into a surveillance mode that may be detected.
3. It is also noted that electricity infrastructure developers do need information to properly design.
4. Make changes to the system and current operating parameters (eg limits) more secure.
5. Move real-time data to more secure access.
6. Is the proper source of information the FERC or the owner of the information?

The CIPAG's response to the CEII NOPR response will be made to the FERC.

### **Critical Spares Initiative** (Open via conference call)

Refer to Motion: 9.

Bob Cummings presented the work of the Security Planning SDWT that is evaluating the need for critical component spares under several scenarios of attack. In a major, multi-city attack there may be need for as many as (just for example of the analysis) 50 transformers of varying sizes together with other kinds of equipment.

In addition to the spares database, work leading toward a gap analysis between needs and availability of spares is proposed. The development of a generic, limited life transformer is underway. Storage and transportation of spares is an issue.

The existing spares database will be enhanced by March 2003. Prevention is very difficult, now. Therefore the recovery planning is critically important.

The project will include a response/recovery plan that will relate to the prevention plans.

Use of the spares in the project to recover from natural disasters would certainly be part of the plan.

There will likely be an initial contract person to serve as project manager for this initiative.

The ultimate cost of this initiative over time may very well be in the order of \$500 million. Funding sources will be part of the project.

Consider review of the industry's nuclear sharing mechanism.  
A project scope document is recommended.

### **National Strategy to Secure Cyberspace**

Tom Flowers reported on the very substantial work done by the National Strategy SDWT on a response to the President's Critical Infrastructure Protection Board on the "National Strategy to Secure Cyberspace". The draft document was presented to the critical infrastructures in September 2002 with a comment period ending 18 November 2002.

There will be a strong recommendation that all National Strategy sections prepared by the critical infrastructures be made available to the recognized ISACs and groups like the CIPAG.

The response document was discussed in some detail; timing has been such that this has not been before the CIPAG long enough to make a final determination at the meeting. It is likely that some additional comments or changes may be recommended by CIPAG members.

Recognizing the timing constraints, the CIPAG established the following plan to submit an approved response to the President's CIP Board:

1. Tom will revise the response based upon comments at this meeting.
2. CIPAG members will send any additional changes to Tom by Monday 11 November 2002 afternoon.
3. Tom will capture any changes and send the revised response to the CIPAG by Tuesday 12 November 2002 morning.
4. CIPAG members will vote yes, no, abstain to Lou Leffler by Thursday 14 November 2002. A quorum and decision will be established from voting roster or roster alternates.
5. In the event of an affirmative vote the response will be submitted by NERC for the CIPAG.
6. In the event an affirmative vote is not reached, it is understood that the NS SDWT may submit a response under its name.

### **CIP Workshops**

Refer to Motion: 5.

As represented in draft-7, the workshops were approved.

### **Public Key Infrastructure Project**

Larry Bugh, Chair of the PKI Project Steering Committee, reported on the meeting held in DC, 30 October 2002. This Committee is staffed with representation from the ES, Oil, and Gas Sectors.

Mitre Corporation is working with the Committee to provide project assistance: technical input to the RFP for Certificate Authorities, incremental deployment strategy for PKI with identified CAs into the process, support to interoperability testing, assist with first annual audit and recertification of CAs that are compliant with the EMARC, some PKI user training.

Follow on PKI Steering Committee tasks include:

1. Complete the architecture with a trust model for use by the industry between users and the CAs.
2. Should there be duplicate certificates for user certification and data assurance?
3. How are individual users authorized to participate with the PKI process?
4. Propose cost allocation.
5. Coordinate with NAESB.
6. Consider making the EMARC document a standard, or doing so by reference.
7. Identify initial industry applications to be PKI enabled.

### **Cyber Log Analysis Project**

Stuart Brindley reported on the pilot project that is underway; there will be discussion at the January 2003 CIPAG meeting. This will focus on learnings, confidentiality issues, next steps.

Scott Mix reported on the Cyber Incident Detection Analysis project.

**Communications SDWT**

The SDWT will continue efforts to assure that the CIP message is getting out broadly. The objective is that all personnel in the ES know of the programs and are in the communications loop or chain from alert/warning initiation to action with appropriate feedback. The ES-ISAC, various in-place and to be established communications, the CIP workshops are all steps in the right direction.

**American Public Power Association (APPA)**

No report.

**Canadian Electric Association (CEA)**

No report.

**Critical Infrastructure Assurance Office (CIAO)**

No report.

**Department of Energy (DOE)**

No report.

**DOE Technology Roadmap**

No report.

**Edison Electric Institute (EEI)**

No report.

**Electric Power Research Institute (EPRI)**

No report.

**Electricity Sector – Information Sharing and Analysis Center (ES-ISAC)**

No report. The ES-ISAC Internet site url is: <<http://www.esisac.com>>

**Federal Energy Regulatory Commission (FERC)**

Covered under Security Standards in the FERC Standard Market Design.

**Information Sharing and Coordinating Group (ISCG)**

No report.

**Joint Projects Office (JPO)**

No report.

**National Infrastructure Protection Center (NIPC)**

No report.

**National Rural Electric Cooperative Association (NRECA)**

No report.

**National Security Agency (NSA)**

No report.

### **Nuclear Regulatory Commission (NRC)**

No report.

### **US Secret Service (USSS)**

Ron Smith, USSS (detailed to the CIAO) presented on the USSS activities that now include protection for all critical infrastructures. There is a focus on cyber incidents. A briefing on the Electronic Crimes Task Force (ECTF) could be made to the CIPAG. There is a designated representative from the USSS to the NIPC. USSS will become part of the Department of Homeland Security.

### **Roundtable**

A pens down roundtable was conducted.

07 November 2002, 16 January 2003  
{min\_cipwg\_07nov2002.doc}

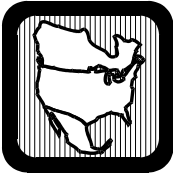
**CRITICAL INFRASTRUCTURE PROTECTION ADVISORY GROUP  
ROSTER  
23 April 2003**

REPR	POSITION	VOTE	NAME	ORGANIZATION	TEL	EML
APPA	Member		Mike Hyland	APPA	202-467-2986	mhyland@APPAnet.org
	Alternate		James Strange	APPA	202-467-2989	jstrange@appanet.org
	Alternate		David S. Behar	Snohomish PUD	425-783-8770	dsbehar@snopud.com
	Member		Doug McKelvey	JEA	904 665-6173	McKeWD@jea.com
	Alternate		James Lauth	Silicon Valley Pwr		jlauth@ci.santa-clara.ca.us
	Alternate		David Godfrey	Texas Municipal Power Agency	936-873-1130	dgodfrey@texasmpa.org
	Alternate		Sandy Brewer	Conway Corp	501-548-3047	sandyb@conwaycorp.net
CEA	Member		Stuart Brindley	IMO	905-855-6108	stuart.brindley@theIMO.com
	Member		Jean-Guy Ouimet	Hydro-Quebec	450-565-0221 ext2232	ouimet.jean-guy@hydro.qc.ca
	Alternate		Seiki Harada	BC Hydro	604-623-3550	Seiki.harada@bchydro.com
	Alternate		Dave Baumken	Hydro One	416-345-4009	david.baumken@Hydroone.com
	Alternate					
NRECA	Member		Paul Butler	Hoosier Energy	812-876-0236	pbutler@hepn.com
	Member		Barry R. Lawson	NRECA	703-907-5781	barry.lawson@nreca.org
	Alternate		Bob Richhart	Hoosier Energy	812-876-0250	richhart@hepn.com
	Alternate					
	Alternate					
ECAR Vice Chair	Member: Phys		Michael Lynch	Detroit Edison	313-235-7733	lynchm@dteenergy.com
Vice Chair	Member: Cybr		Larry Bugh	ECAR	330-580-8017	larryb@ecar.org
	Member: Oper		Scott Moore	AEP	614-716-6600	spmoore@aep.com
	Alternate: Phys					
	Alternate: Cybr		Frank Dessuit	NIPSCO	219-853-5217	fdessuit@NiSource.com
	Alternate: Oper					
	Alternate: Cyber		Jerry Freese	AEP	614-716-2351	gsfreese@aep.com
	Alternate: Cyber		Paul Castellano	Allegheny Power	724-838-6850	pcastel@alleghenypower.com
	Alternate: Phys		Scott Webber	Allegheny Power	724-838-2324	swebber@alleghenypower.com
	Alternate: Phys		Ted Almay	AEP	614-716-3020	talmay@aep.com
	Alternate: Phys		Jim Miller	NiSource	219-647-5706	jpmiller@nisource.com

REPR	POSITION	VOTE	NAME	ORGANIZATION	TEL	EML
	Alternate: Phys		Joe Douthitt	LGE Energy	502-627-2454	joe.douthitt@lgeenergy.com
ERCOT	Member: Phys		Bill Bojorquez	ERCOT	512-248-3036	bbojorquez@ercot.com
	Member: Cybr		Chris Uranga	ERCOT	512-248-3092	curanga@ercot.com
	Member: Oper		Steve Myers	ERCOT	512-248-3077	smyers@ercot.com
	Alternate: Phys		Lewis R. Griffith	CenterPoint Energy	713-207-7422	lewis.griffith@centerpointenergy.com
	Alternate: Phys		David L. Andrews	TXU Business Services	214-812-8964	dandrew1@txu.com
	Alternate: Cybr		Luis Quintanilla	ERCOT	512-248-3157	lquintanilla@ercot.com
	Alternate: Cybr		Tom Flowers	CenterPoint Energy	713-207-2122	tom.flowers@centerpointenergy.com
	Alternate: Oper		John Adams	ERCOT	512-248-3130	jadams@ercot.com
	Alternate					
FRCC	Member: Phys		Frank Prieto	FPL	305-442-5804	frank_prieto@fpl.com
	Member: Cybr		Brian Malfant	FRCC	813-289-5644	bmalfant@frcc.com
	Member: Oper		Chuck Harper	Progress Energy - Florida	727-384-7819	charles.harper@pgnmail.com
	Alternate: Phys		Robert Champion	Progress Energy	919-546-5330	robert.champion@pgnmail.com
	Alternate: Cybr					
	Alternate: Oper		Linda Campbell	FRCC	813-289-5644	lcampbell@frcc.com
	Alternate					
MACC	Member: Phys		Robert H. Beahm	BGE	410-597-7777	robert.h.beahm@bge.com
	Member: Cybr		John Maguire	PJM	610-666-4420	maguij@pjm.com
	Member: Oper		Walter A. Johnson	PEPCO Holdings	410-469-5252	wajohnson@pepco.com
	Alternate: Phys		R. Scott Heffentrager	PJM	610-666-2222	heffens@pjm.com
	Alternate: Cybr		Robert Farrington	PECO	215-841-6301	robert.farrington@exeloncorp.com
	Alternate: Oper		Frank Koza	PJM	610-666-4228	kozaf@pjm.com
	Alternate					
MAIN	Member: Phys		Pat Laird	Exelon	312-394-8553	patrick.laird@exeloncorp.com
	Member: Cybr		Roger Kizior	WPS	920-433-2237	rkizior@wpsr.com
	Member: Oper		Eric Solberg	ATC	262-506-6746	esolberg@atcllc.com
	Alternate: Phys					
	Alternate: Cybr					
	Alternate: Oper		Len Januzik	MAIN	630-261-2611	lrj@maininc.org
	Alternate					

REPR	POSITION	VOTE	NAME	ORGANIZATION	TEL	EML
MAPP	Member: Phys		Scott McCoy	XCEL Energy	612-330-7666	Richard.S.McCoy@xcelenergy.com
	Member: Cybr		Greg Fraser	Manitoba Hydro	204-487-5379	gjfraser@hydro.mb.ca
	Member: Oper		Dave Kulisek	Omaha Public Power District	402-515-1005	dkulisek@oppd.com
	Alternate: Phys					
	Alternate: Cybr					
	Alternate: Oper					
	Alternate					
NPCC	Member: Phys		Ronald P. Belval	Vermont Elec Pwr	802-770-6333	rbelval@velco.com
	Member: Cybr		Chuck Noble	ISO New England	413-540-4232	cnoble@iso-ne.com
	Member: Oper		Roger Lampila	New York ISO	518-356-6043	rlampila@nyiso.com
	Alternate: Phys		Bruce Metruck	New York PA	315-792-8213	metruck.b@nypa.gov
	Alternate: Cybr		Brian Hogue	NPCC	212-840-1070	bhogue@npcc.org
	Alternate: Oper					
	Alternate		Bonnie Bushnell	New York ISO	518-356-6238	bbushnell@nyiso.com
SERC	Member: Phys		Robert D. Canada	Southern Co Svcs	404-506-5145	rdcanada@southernco.com
	Member: Cybr		Jay S. Cribb	Georgia Pwr Co	404-506-3854	jscribb@southernco.com
	Member: Oper		Carl J. Eng	Dominion	804-273-3305	Carl_Eng@dom.com
	Alternate: Phys		Terrence P. Luddy	Duke	704-382-6462	tpluddy@duke-energy.com
	Alternate: Cybr		Tim Brown	Southern Co Svcs	205-257-4537	ctbrown@southernco.com
	Alternate: Oper		Gene Byars	Southern Co Svcs	205-257-3303	epbyars@southernco.com
	Alternate					
SWPP	Member: Phys		Larry Dolci	Great Plains En	816-654-1661	larry.dolci@kcpl.com
Chair	Member: Cybr		Kevin B. Perry	SWPP	501-614-3251	kperry@spp.org
	Member: Oper		Allen Klassen	Westar Energy	785-575-6073	allen_klassen@wr.com
	Alternate: Phys		Walt Wilhelm	Oklahoma G&E	405-553-3387	wilhelw@oge.com
	Alternate: Cybr		Joe Doetzi, Sr	Great Plains En		joe.doetzi@kcpl.com
	Alternate: Oper		Tom Stuchlik	Westar Energy	785-575-6046	tom_stuchlik@wr.com
	Alternate					
WECC	Member: Phys		Robert Windus	BPA	503-230-5148	rlwindus@bpa.gov
	Member: Cybr		James Sample	Cal ISO	916-608-5891	jsample@caiso.com
	Member: Oper		Dennis E. Eyre	WECC	801-582-0353	Dennis@wecc.biz
	Alternate: Phys		Robert L. Sypult	So Cal Edison Co	626-302-7910	Robert.Sypult@sce.com
	Alternate: Phys		Lyman H. Shaffer	Pacific G&E	415-923-6920	LHS1@pge.com

REPR	POSITION	VOTE	NAME	ORGANIZATION	TEL	EML
	Alternate: Cybr					
	Alternate: Oper		Thomas Glock	Arizona Pub Serv	602-250-1160	thomas.glock@aps.com
	Alternate: Oper		Jack Bernhardsen	PNSC	360-418-2956	jack@pnsc-center.com
NERC	Staff Support		Lyn Costantini	NERC	609-452-8060	lynn.costantini@nerc.net
	Staff Support		Ron Niebo	NERC	609-452-8060	ron.niebo@nerc.net
	Staff Support		Lou Leffler	NERC	609-452-8060	lou.leffler@nerc.net



## NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

### Critical Infrastructure Protection Advisory Group Scope

#### Mission

The mission of the Critical Infrastructure Protection Advisory Group (CIPAG) is to advance the physical and cyber security of the critical electricity infrastructure of North America.

#### Activities

1. Serve as an expert advisory panel to the NERC Board of Trustees and Standing Committees in the areas of physical and cyber security.
2. Serve as an expert advisory panel to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) including the ES-ISAC's role in implementing the Indications, Analysis, and Warnings Program.
3. Coordinate and communicate with those responsible for both physical and cyber security in all electric industry segments, including (among others) the American Public Power Association, Canadian Electricity Association, Edison Electric Institute, Electric Power Research Institute, Electric Power Supply Association, National Rural Electric Cooperative Association, North American Energy Standards Board, the Nuclear Energy Institute, and the NERC Regions.
4. Coordinate and communicate with the other critical infrastructure sectors as appropriate.
5. Liaison with federal government agencies charged with critical infrastructure protection.
6. Establish and maintain an information reporting procedure for critical infrastructure protection among industry segments and, as appropriate, with federal government agencies.
7. Develop Security Guidelines.
8. Conduct forums and workshops related to the scope of CIPAG.

The essential work of the CIPAG regarding the Electricity Sector include the following actions:

- ✓ **Protection** — includes physical security, cyber security, emergency preparedness and response, business continuity planning, and recovery from a catastrophic event, with emphasis on deterring, preventing, limiting, and recovering from terrorist attacks.
- ✓ **Deterring** — to dissuade one from even trying.
- ✓ **Preventing** — to cause an attempt to fail.
- ✓ **Limiting** — to constrain consequences in time and scope to something less than what they would have been otherwise. And,
- ✓ **Recovering** — returning to normalcy quickly and without unacceptable consequences in the interim.

#### Reporting

The CIPAG reports to the NERC Board of Trustees.

Approved by CIPAG: January 17, 2003

Approved by Board of Trustees: February 11, 2003

## Voting Members

- 2 selected by the American Public Power Association
- 2 selected by the Canadian Electricity Association
- 2 selected by the National Rural Electric Cooperative Association
- 30 **Each** of the ten NERC Regions will appoint three members, one each with expertise in Physical Security, Cyber Security, and Operations as defined below.
- If other entities not represented in this model request representation, the request will be considered at the next CIPAG meeting and subject to NERC Board approval.

There will be a total of 36 voting members.

- The chair and two vice chairs will be appointed by the NERC Board from among the voting members.
- Regional representation will be appointed by each of the ten Regional Councils.
- Members will be selected based upon expertise in these disciplines:
  - ✓ **Physical Security** of Electricity Sector facilities (including, not limited to, generation, dams, transmission, critical distribution facilities, buildings).
  - ✓ **Cyber Security** primarily focused on Market and Power Operations Systems (including, but not limited to, SCADA, EMS, DCS, and also systems like OASIS), but with consideration also to systems required for business continuity.
  - ✓ **Operations** with focus on system operations at the control area (balancing authority) and reliability coordinator levels.
- Appropriate representation will be provided to deal effectively with **Policy Matters** related to electricity industry evolution and government policy.

## Nonvoting Members

- Governmental agencies at the national, provincial, and state levels
- Other electricity industry associations
- Electric Power Research Institute
- Vendors
- Other critical infrastructure protection sectors
- Other observers as appropriate
- CIPAG secretary
- NERC committee meetings are open, with the understanding that certain discussions may, as ordered by the chair, be held in closed session limited to the voting members and secretary.
- Nonvoting members have voice at meetings

## Structure

The CIPAG shall have an Executive Committee with the following membership:

- Chair
- Vice Chairs
- One CIPAG member (appointed by the chair with consent of the members) representing each:
  - ✓ Physical Security
  - ✓ Cyber Security
  - ✓ Operations
  - ✓ Policy Matters
- Secretary

Executive Committee duties:

1. Respond to urgent matters by calling conference calls or special meetings
2. Prepare meeting agendas
3. Coordinate CIPAG activities with NERC standing committees and other entities
4. Report to the NERC Board of Trustees

The CIPAG may address security-related issues as it deems fit or may assign such issues to self- directed work teams.

Self-directed work teams will take assignments from the CIPAG and all work products will be presented to the CIPAG for any further action.

The CIPAG will transition from its existing structure to that detailed in this scope, for a one-year period, following review for approval of the NERC Board at its February 2003 meeting. This structure will be reviewed by the CIPAG and NERC committee(s) with a detailed report prepared by the CIPAG presented to the NERC Board by February 2004.

Terms of chair, vice chair(s), and members will be determined during the transition.

### **Governance**

1. Roberts Rules of Order will apply.
2. A CIPAG quorum requires 50% of the voting roster members to be present or represented by proxy. Any or all members of the CIPAG may participate in a meeting, including being counted as part of the quorum, by means of a communication system by which all persons participating in the meeting are able to hear each other.
3. Motions carry upon affirmative vote of two-thirds of the total yes and no votes cast during the presence of a quorum. Abstentions do not count as votes.
4. Only roster alternates may be designated as proxy representatives who may attend and vote at meetings provided the absent member notifies in writing (letter, facsimile, or e-mail) the chair, vice chair, or secretary. The proxy representative and his or her affiliation shall also be named in the correspondence. Any person, member or proxy, will have one vote; no regular voting member of CIPAG may hold a proxy for another member.
5. The agenda of actions to be voted upon shall include the general wording of proposed motions, and a brief discussion of the reasons for the motion. Motions can be made during a meeting or conference call. Only a voting member can provide a motion. A reasonable effort shall be made by those sponsoring items on a meeting agenda to have the action to be voted on and with background material distributed with the agenda or in a timely manner before the meeting.
6. CIPAG may take action without a meeting if, after notice to all members, two-thirds of the members consent to the action in writing. Such action without a meeting shall be performed by electronic (facsimile or e-mail) ballot. The Executive Committee may initiate the call for such an action. Any member may ask the chair to arrange for such an action.
7. On occasion, the CIPAG may be called upon to provide information or support in relation to a matter that requires secrecy. Upon such an occasion and with the approval of the chair of the Board of Trustees, the chair of the CIPAG may convene a working group to provide such information or support without notice or approval of any other member or group. The existence of such a working group, its mission and results, will be shared with the members only to the degree and at the time deemed appropriate by the chair of the Board of Trustees.
8. The CIPAG will coordinate its activities with the other NERC committees and working groups to assure the highest degree of collaboration possible.
9. CIPAG actions, documents, and recommendations will be distributed to the NERC committees and working groups and posted for Industry comment (assuming sensitivity so permits, at the discretion of the CIPAG). NERC committee, working group, and industry comments will be considered by the CIPAG prior to forwarding actions or documents to the Board for approval.
10. CIPAG meetings will be conducted at the discretion of the chair, generally on a quarterly basis.

**ELECTRICITY SECTOR (ES)  
CRITICAL INFRASTRUCTURE PROTECTION ADVISORY GROUP (CIPAG)  
TASK FORCES**

07 January 2003

**Active**

1. **Standard Operating Procedure Task Force**
  - A. Maintain the NERC-NIPC Indications, Analysis, Warnings (IAW) Program.
  - B. Harvey Blumenthal, Tom Bowe, Stuart Brindley, Jack Bernhardsen, Glenn Coplon, Michael Cohen, Wally Johnson, Kevin Perry, Roger Lampila, Chuck Noble, Larry Dolci, Larry Bugh, Joe Gracia, Hector Alvarez, Herman Green, Scott Mix
2. **Cyber Incident Task Force**
  - A. Adjust the IAW cyber incident definitions.
  - B. Carl Eng, Larry Dolci, Joe Doetzl, Chuck Noble, Kevin Perry, Glenn Coplon, Jeff Dagle, Michael Cohen
3. **Reporting Mechanisms Task Force**
  - A. Develop specific reporting means to alert the ES entities and disciplines of Alert Levels and security measures.
  - B. Crisis Response System.
  - C. Scott Mix, Larry Bugh, Harvey Blumenthal, Michael Cohen, Bonnie Bushnell, Lynn Costantini, Lou Leffler
4. **Communications Task Force**
  - A. Prepare, administer, and provide training in security measures (including the IAW Program) for the ES.
  - B. Wally Johnson, Joe Gracia, Glenn Coplon, Mike Hyland, Brian Malfant, Nancy Wong, Jim Fortune, Mike Hagee, Eric Solberg
5. **Approach to Action Task Force**
  - A. Maintain the ES Approach to Action (for Security) document.
  - B. Jim Fortune, Nancy Wong, Craig Zingman, Stuart Brindley, Joe Gracia, Herman Green
6. **National Strategy Task Force**
  - A. Propose and maintain the ES input to the US National Strategy.
  - B. Tom Flowers, Herman Green, Gene Byars, Jerry Freese, Roger Lampila, Scott Mix, Kurt Muehlbauer, Chuck Noble, Lyman Shaffer, Tom Benton, Craig Zingman, Larry Brown, Joe Weiss, Lou Leffler
7. **PKI Task Force**
  - A. Develop the Public Key Infrastructure for the ES.
  - B. Larry Bugh, Chuck Noble, Scott Mix, Todd Kochheiser, NERC Staff
8. **Security Guides Task Force**
  - A. Propose a Security Guides structure and specific guides for consideration.
  - B. Randy Mayfield, Herman Green, Mike Lynch, Kimberly Denbow, Chuck Noble, Kevin Perry, Bob Sypult, Lyman Shaffer, Lyn Costantini

9. **Electricity Sector Information Sharing and Analysis Center Task Force**
  - A. The ES-ISAC SDWT will conduct the CIPAG Scope activity to provide guidance to the ES-ISAC development.
  - B. Michael Lynch, Joe Gracia, Chis Curtis, Scott Mix, Stuart Brindley, Kevin Perry, Wally Johnson, Eric Solberg, Larry Bugh, Ted Heller, Chuck Noble, Gene Byars, Lou Leffler
  
10. **Business Case Task Force**
  - A. Write and maintain security awareness materials for the ES.
  - B. Nancy Wong, Jim Fortune
  
11. **Security Planning Task Force**
  - A. Develop ES planning responses to the new threats. Develop the Critical Spares Database. Spares gaps analysis, EPRI infrastructure security initiatives.
  - B. Michael Innocenzo, Don Covalleski, Michael Lynch, Paul Johnson, John Riley, Lee Westbrook, Mike Green, Bill Harm, Bruce Renwick, Don Volzka, Larry Brusseau, Karl Tammar, Doug Powell, Perry Stowe, Chuck Chakravarthi, Michael Hagee, James Sample, Malcolm V. Thaden, Jr., Mike Gevaza, Mike DeLaura, Bob Cummings
  
12. **FERC Assist Task Force**
  - A. Work with the FERC and CIPAG to develop (primarily) Cyber Security Standards for the Standard Market Design.
  - B. Chuck Noble, Michael Lynch, Larry Bugh, Kevin Perry, Jeff Dagle, Herman Green, Roger Lampila, Mike Peters, Stuart Brindley, James Sample, Eric Solberg, Mike Hagee, James Strange, Lyn Costantini
  
13. **CIPAG Organization Task Force**
  - A. Develop a revised Scope for the CIPAG. The Scope will include duties, membership, voting, CIPAG functioning mechanics.
  - B. Michael Lynch, Co-Chair, Bob Sypult, Co-Chair, Bob Beahm, Larry Brown, Larry Bugh, Gene Byars, Linda Campbell, Bob Canada, Ron Dollin, Phil Donegan, Dundeeana Doyle, Tom Flowers, Bill Flynt, Jim Fortune, Jerry Freese, Floyd Gavin, Ronnie Goebel, Sergio Guzman, Mike Hagee, Ken Hall, Carman Hutmacher, Mike Hyland, Pat Laird, Barry Lawson, Randy Mayfield, Scott McCoy, Kevin Perry, Jamey Sample, Lyman Shaffer, Lyn Costantini, Lou Leffler
  
14. **Process Controls Security Task Force**
  - A. Develop plan to secure PCS in the short and long term on a cross-Sector basis with PCS Vendor participation.
  - B. Prepare Security Guidelines for PCS and present to the CIPAG for approval to submit to the NERC Board.
  - C. Scott Mix, Catherine Cook, Steve Harp, David Saunders, Gene Byars, Homer Cotton, Kevin Perry, Rick Morse, Tariz Samad, Andy Turke, Allen Risley, Tom Kropp, Jim Fortune, Joe Weiss, Lou Leffler
  
15. **CIP Workshops Task Force**
  - A. Plan, conduct, and modify as necessary a series of CIP Workshops for the Electricity Sector.
  - B. Larry Brown, Bill Flynt, Herman Green, Ken Hall, Mike Hyland, Wally Johnson, Pat Laird, Barry Lawson, Michael Lynch, George Miserendino, Lyman Shaffer, Lou Leffler

**Inactive**

1. **Industry Acceptance (of the Approach to Action) Task Force (roll into communications)**
  - A. Promote the ES Approach to Action (for Security).

B. Larry Brown, Wally Johnson, David Cook, Stuart Brindley, Mike Hyland, Larry Dolci

2. **Security Alerts Task Force**

A. Write Security Threat Alert Levels and Guidelines for Physical, Cyber, Operations. Propose secure telecommunications.

B. Prepare for OHS Homeland Security Advisory System.

C. Chuck Noble, Hector Alvarez, Michael Cohen, Bob Windus, Bill Flynt, Bryan McMillan, Lyman Shafer, James Sample, Gene Byars, Michael Lynch, Jim Mackey, Jim Baker, Lou Leffler

3. **CIP Data Task Force**

A. Develop approach to security for sensitive Electricity Sector data and information.

B. Review with guideline and policy for NERC data/information.

C. Stuart Brindley, Wally Johnson, Larry Bugh, Larry Dolci, James Sample, Craig Zingman, Bryan McMillan, Jim Baker, Lou Leffler

4. **Computer Based Training Task Force**

A. Develop training materials for the IAW Program.

B. Herman Green, Jack Bernhardsen, Greg Campbell, Scott Mix, Michael Cohen

**Task Completed**

1. **InfraGard Agreement Task Force**

A. Assist in development of the FBI InfraGard participation agreement.

B. Brett Hovington, David Cook, Larry Brown, Larry Bugh

(First named is convener.)

{cipag\_sdwt.doc}

# **ELECTRICITY SECTOR CRITICAL INFRASTRUCTURE PROTECTION COMMUNICATIONS**

18 April 2003

## **Purpose**

These communications are intended to assure awareness of critical infrastructure protection issues and PARTICULARLY immediate dissemination of threat advisories to the Electricity Sector (ES) to assist the sector to take prompt, appropriate actions to protect:

- Physical Security
- Cyber Security
- Operations.

Threat advisories may be on a National, Sector, Geographic Area, Specific Facility basis. The Electricity Sector – Information Sharing and Analysis Center (ESISAC) will notify the ES and/or, as appropriate, specific organizations.

The ESISAC communicates with the Department of Homeland Security (DHS) Information Analysis and Infrastructure Protection (IAIP) Division, the Department of Energy, and other Agencies and has secure and redundant communications facilities.

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

- Receive ES information for analysis by Government Agencies and the ISAC.
- Provide analytical support to the DHS and other Government Agencies in the interpretation of information relevant to the ES.
- Promptly disseminate threat indications, analyses, warnings together with interpretations to assist the ES in taking protective actions.

A key program for information sharing is the NERC-DHS Indications, Analysis, Warnings program (IAW).

The ESISAC seeks opportunities to address Electricity Sector meetings to help raise and maintain awareness to the critical infrastructure protection issues, proposed solutions, and (future) standards. A series of CIP workshops are being conducted throughout the US and Canada during 2003: <http://www.nerc.com/~filez/cipworkshop.html>.

## **Reference Documents**

These documents are available via the ESISAC Internet site:

<http://www.esisac.com>

1. NERC-DHS IAW Program
2. Security Guidelines
3. Threat Alert Levels-Physical
4. Threat Alert Levels-Cyber
5. Approach to Action
6. Business Cases for Action

## **Communications**

InfraGard is an approach to sharing security practices among program participants. This program is operated from each FBI field office. The InfraGard secure telecommunications can be used to communicate with the IAW Program. Contact the local FBI office for details.

CIPIS is a secure Internet messaging system operated by the ESISAC for communications with the DHS and the ESISAC and among ESISAC participants. A user of the CIPIS must register and be authenticated as a valid participant with the ESISAC. There are no fees. Registration can be initiated via: <<https://www.nerc.net/registration/>>

Enter all requested information including your own desired User Name and Password combination. ESISAC staff will affirm user authentication; a confirming email message will be sent to the registrant.

The CIPIS is accessed using an Internet browser via: <<https://www.nerc.net/cip/>>  
(Note the https, which indicates a secure connection is being used.)

Threat Advisory List (TAL) is an email listserver used to distribute CIP messages and reports to those involved in Physical Security, Cyber Security, Operations from the DHS, the ESISAC, and others. Included communications are DHS Daily Watch reports, ESISAC Threat Levels and messages, forwarded messages from organizations such as the CERT. (Note that pagers and cell phones, that can be addressed via email, can be included on the TAL.)

ESISAC Internet Site <<http://www.esisac.com>> contains all CIP related documents. All current applicable Threat Levels are posted (Homeland Security Advisory, ES-Physical, ES-Cyber, DOE, NRC). Other information includes contacts and links to other security Internet sites.

### **Contacts**

1. Please note that the initial emergency or incident event report should be to Local Law Enforcement and Local FBI. These relationships should be in place.
2. It is essential that prompt and effective communications within an organization are in place with periodic testing. Alerts must be communicated to those expected to take action whenever a Physical or Cyber Threat Level change is initiated or a specific threat is received.
3. DHS, IAIP
  - A. Email: [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov)
  - B. Tel: 202-323-3204,5,6  
888-585-9078
  - C. Fax: 202-323-2079, -2082
4. ESISAC
  - A. Email: [esisac@nerc.com](mailto:esisac@nerc.com)
  - B. Tel: 609-452-8060 (NERC office hours)
  - C. Tel: 609-452-1422 (routes to cell phone: all hours)
  - D. Pager: 800-582-4419
  - E. Pager  
via Email: [5824419@skytel.com](mailto:5824419@skytel.com)
  - F. Fax: 609-452-9550
  - G. STU: 609-452-0689
  - H. Internet: <http://www.esisac.com>

## **REPORT INCIDENTS TO:**

### **1. LOCAL LAW ENFORCEMENT**

Establish and maintain relationship

### **2. LOCAL FBI**

Establish and maintain relationship

### **3. DHS-IAIP IAW Program**

InfraGard; CIPIS; [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov);

202-323-3204,5,6;

888-585-9078

### **4. ESISAC**

CIPIS; [esisac@nerc.com](mailto:esisac@nerc.com);

609-452-8060 [day];

609-452-1422 [anytime]

# Meeting The Security Challenge Workshop

[Proceed to Registration](#)

Protecting the electric power systems from disruption is essential – no one disputes the point. Given today’s threat environment, the question is how? Physical and cyber assets are at risk. Threats lurk inside the organization as well as out. Vulnerabilities exist.

NERC is sponsoring workshops across the US and Canada to help address the question of how to protect our critical infrastructure. The Security Guidelines for the Electricity Sector, developed by NERC’s Critical Infrastructure Protection Advisory Group last year, will be the cornerstone of discussion.

Subject matter experts from the industry and U.S. government will present the guidelines, discuss NERC’s proposed Cyber Security Standard, and describe tools and assessment techniques available today to help electricity sector organizations determine vulnerabilities and define effective protection strategies.

If you have responsibility in the physical or cyber-security areas or operations, plan on attending a workshop. The dates and locations have been selected to allow you to choose the most convenient schedule.

## The Agenda

<b>Day 1 - 8:00 a.m. - Noon</b>
Welcome
Workshop objectives and agenda
North American Electric Reliability Council (NERC); Critical Infrastructure Protection Advisory Group (CIPAG); Electricity Sector-Information Sharing and Analysis Center (ES-ISAC)
Electricity Sector (ES) Security Guidelines <u>Overview</u> : Approved Security Guidelines: Physical, Cyber Draft Security Guideline: Electronic Controls Draft Security Guideline: Incident Reporting Proposed Cyber Security Standard
Luncheon: Speaker
<b>Day 1 - 1:15 p.m. - 5:00 p.m.</b>
Security Guidelines – Physical: Breakout discussion Security Guidelines – Cyber: Breakout discussion

<p>Homework Assignments! Self Assessment: Overview and Exercise</p> <p>Threat Alert Levels for the ES – Physical and Cyber: Overview and Exercise</p>
Reception: 5:30 p.m. – 7:00 p.m.
<b>Day 2 - 8:00 a.m. - Noon</b>
Exercises Review
Overall Q&A
Communications: Indications, Analysis, Warnings Program; ES-ISAC
<p>Assessment Methodologies:</p> <ul style="list-style-type: none"> <li>- DHS Vulnerability Assessment Methodology</li> <li>- Risk Assessment Methodologie RAM)</li> <li>- Red, Gray, Blue Self-Assessment Methodology</li> <li>- System-X Assessment Experience</li> </ul>
Workshop Wrap-up: On-going work within the ES to help assure security; review contacts; feedback

## The Presenters

- NERC CIPAG
- ES-ISAC
- U. S. Department of Homeland Security

## The Schedule

Date (2003)	Location
February 26-27	Dallas, TX
March 13-14	Phoenix, AZ
March 27-28	Seattle, WA
April 10-11	Washington, D.C.
April 24-25	Orlando, FL
29-30 May	Denver, CO
18-19 June	Chicago, IL
24-25 July	Boston, MA
<i>Other locations will be added as needed</i>	

## The Registration Process

The workshop registration fee is \$125 per person. This price includes meeting facilities, materials, and refreshments. Please pre-register - registration at the door is \$175. NERC will accept registrations, cancellations and substitutions one week prior to the session. To register for the ***Meeting the Security Challenge Workshop***, click the link below. Direct questions to [Paulette Garcia](#), 609-452-8060.

# Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems

NERC	Guideline
<b>Guideline Title: Securing Remote Access to Electronic Control and Protection Systems</b>	<b>Status: DRAFT, 16 January 2003</b>
<b>Guideline Number: NERC-Guideline- {#}</b>	<b>Version: 0.3.1</b>
Contact: Scott Mix	Effective Date:
	Revision Date:

## **Purpose:**

The purpose of this guideline is to describe minimum recommendations for securing Remote Access associated with Electronic Control and Protection Systems (ECPS). This guideline identifies some of the key elements associated with managing remote access to ECPS to help ensure reliability of the Electricity Infrastructure.

## **Applicability:**

This guideline is focused on ECPS remote access other than that provided for by the primary exchange of real-time data and control signals.

This guideline is applicable to anyone who owns, manages, or maintains ECPS and/or services that support the Electric Infrastructure.

A computer system environment is as critical as its most critical component and as vulnerable as its most vulnerable component. Therefore this guideline would be applicable across the enterprise.

## **Background:**

ECPS control the systems that generate, transmit, and distribute electricity. For business reasons, it is necessary to provide a means for users to remotely access ECPS. Remote Access to these systems may require special considerations for security. Unauthorized Remote Access to an ECPS can result in interruption of electric service, damage to the elements of the electric grid, or a danger to life and property. ECPS vendors and other support personnel increasingly use Remote Access tools such as pcAnywhere™, telnet, and FTP for support purposes directly over the Internet to the internal controls networks.

As a result, it is critical to preserve the security of the Remote Access to the ECPS. Authentication of the user is a critical element of the security policy.

# Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems

## Definitions:

### Electronic Control and Protection Systems:

Those systems used to regulate physical processes, including but not limited to: electronic protective relays, substation automation and control systems, power plant control systems, energy management systems (EMS), supervisory control and data acquisition (SCADA), programmable logic controllers (PLC). ECPS attributes include a Time Critical nature and automated response.

### Remote Access:

Access to an ECPS by anything other than a directly connected operations system.

Includes, for example, the functions of administration, diagnostics, configuration, non-operator observation, and non-routine or infrequent control.

Includes, for example, applications such as telnet, SSH, and remote desktop software such as pcAnywhere™, Dameware™, VNC™. Currently available operating systems may natively include this type of functionality.

Includes all private and public telecommunications links, for example, dial-up modem, frame relay, ISDN, public switched telephone network, leased line, microwave, fiber optic, Internet, wireless.

### Time Critical:

Involves a specific bounded time window within which one or more specified actions must be completed with some defined level of certainty.

## Guideline Statement:

Effective and secure Remote Access controls are critical to protecting ECPS. Anyone who owns, maintains, or manages ECPS should have documented policies and procedures in place to manage authorization, authentication, and monitoring of remote access to such systems and devices. Such documentation should clearly define roles, responsibilities, and procedures for establishing authorization, and the methods selected for electronic access, authentication, and monitoring.

The details included in this security guideline can generally be implemented with currently available technology.

# **Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems**

## **Guideline Detail:**

1. Policies and procedures governing use and installation of Remote Access for ECPS, including identifying responsible parties, should be established. These should be reviewed periodically and updated as required.
2. Remote Access should only be enabled when required, approved, and authenticated.
3. Multi-factor (two or more) authentication should be used. Factors include something “you know” (for example: passwords, destination IP address and/or telephone number), something “you have” (for example: token, digital certificate), something “you are” (for example: biometrics). Other factors may include: source IP address and/or telephone number, GPS location. These will make access more difficult for unauthorized users and will help to ensure identity of authorized Remote Access users.
4. Automatically lock accounts or access paths after a preset number of consecutive invalid password attempts. Consider automatically unlocking the account or access path after a pre-determined period of time or by other methods to ensure safe and reliable system operations.
5. Encryption should be used when traversing unsecured networks to gain Remote Access. This will help ensure confidentiality and integrity of any information transfer.
6. Approved Remote Access authorization lists should be established. These lists should be reviewed periodically and updated as required.
7. Change or delete any default passwords or User IDs. Consider using meaningful but non-descriptive IDs.
8. All Remote Access enabling hardware and software should be approved and installed in accordance with Policy. The location and specification of Remote Access enabling hardware and software should be documented and maintained in a controlled manner. Periodic audits should be conducted to ensure compliance.
9. Remote Access connections should be logged. Logs should be periodically reviewed.
10. Consider risk to the process when allowing Remote Access and specifying hardware and software.

# **Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems**

11. Policy considerations for Remote Access modems:
  - A. Change default settings as appropriate:
    - a. Set dial-out modems to not auto answer.
    - b. Increase ring count before answer.
    - c. Utilize inactivity timeout if available.
  - B. Change passwords periodically.
  - C. Use callback whenever possible.
  - D. Require authentication before connection.
  - E. Make maximum use of available security features.

## **Exceptions:**

This security guideline does not pertain to real time transfer of data and control commands.

This security guideline does not address the integrity or confidentiality of the data on the device or of communications to the device.

This security guideline does not address measures to preserve the availability of the device (i.e., measures to protect against denial of service attacks).

There may be some legacy ECPS for which it is technically infeasible to apply all of the specifics contained in this security guideline.

## **Related Documents:**

Internet sites:

Electricity Sector Information Sharing and Analysis Center  
(<http://www.esisac.com>)

The SANS (System Administration, Networking, and Security) Institute  
(<http://www.sans.org>)

The Open Web Application Security Project (OWASP)  
(<http://www.owasp.org>)

The National Security Agency  
(<http://www.nsa.gov/snac/index.html>)

The Center for Internet Security (CIS)  
(<http://www.cisecurity.org>)

# Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems

The National Infrastructure Protection Center  
(<http://www.nipc.gov/publications/publications.htm>)

National Institute of Standards and Technology  
(<http://csrc.nist.gov/publications/nistpubs/index.html>)

U.S. government's CIO Council  
(<http://bsp.cio.gov/>)

The Cyber Emergency Response Team  
(<http://www.cert.org/>)

## Revision History:

Date	Version Number	Reason/Comments
06 Nov 2002	Version - 0.1	Initial draft.
03 Jan 2003	Version – 0.2	Comments from initial external review.
16 Jan 2003	Version – 0.3.1	Final review by SDWT.

# Security Guidelines for the Electricity Sector: Threat and Incident Reporting

<b>NERC</b>	<b>Guideline</b>
<b>Guideline Title: Threat and Incident Reporting</b>	<b>Status: DRAFT, January 31, 2003</b>
<b>Guideline Number: NERC-Guideline- {#}</b>	<b>Version: 0.9</b>
Contact: Stuart Brindley	Effective Date:
	Revision Date:

## **Purpose:**

Each organization should consider having a timely and effective reporting process for communicating security threats or incidents affecting their critical physical and cyber infrastructure. Such threats or incidents can include acts of a criminal, terrorist or cyber disruption. The purpose of this guideline is to describe this reporting process and encourage organizations to promptly report suspicious activities, threats or acts of sabotage, vandalism or terrorism. An effective reporting process will ease the burden on operations staff by enabling the appropriate involvement of the organization's physical or cyber security and emergency management personnel, as well as industry, regulatory, government and law enforcement organizations.

This security guideline does not pertain to communications and reporting procedures required for the real-time operation of electricity markets and grid operations.

While the reporting processes described are voluntary and will vary depending on the role of the organization in the electricity industry, it is the intent that such a reporting process would enable organizations to respond rapidly to the security threat or incident, and provide others outside the organization with information needed to provide assistance or take independent action.

This voluntary guideline encourages organizations to report significant security threats or incidents to the Electricity Sector – Information Sharing and Analysis Center (ES-ISAC). The ES-ISAC<sup>1</sup> is operated by NERC and serves the electricity sector by facilitating communications between electricity sector organizations, U.S. and Canadian federal governments and other critical infrastructure industries. The ES-ISAC promptly disseminates threat indications, analyses and

---

<sup>1</sup> [www.es-isac.com](http://www.es-isac.com)  
Version Number: 0.9  
January 31, 2003

# **Security Guidelines for the Electricity Sector: Threat and Incident Reporting**

warnings, together with its interpretations, to assist electricity sector organizations to take protective actions.

## **Applicability:**

This guideline is intended to focus on reporting suspected or overt attacks of a physical or cyber nature with the potential to significantly affect reliable power system or market operation.

This guideline applies to entities that own or operate facilities and perform functions that are considered critical to the operation of the electricity market and power system, or critical to the overall operation of the individual organization.

A critical facility may be defined as any facility or combination of facilities, that if severely damaged or destroyed, would have a significant impact on the ability to serve large numbers of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the energy grid or would cause significant risk to public health and safety.

This guideline does not supercede or replace reporting processes required for real-time power system or market operation, or as required by law. For example, organizations should have in place processes to report significant incidents affecting the bulk electric power system to their NERC reliability coordinator, who, in turn, would communicate this information with other NERC reliability coordinators across North America. The NERC reliability coordinator is responsible for ensuring the reliability of the bulk power transmission system within its reliability coordinator area, and is therefore in a position to assess the risks and call for emergency control actions such as redirecting generator dispatch, recalling transmission or generator outages, purchasing emergency energy, invoking public appeals for load reduction or implementing load shedding.

## **Guideline Statement:**

This guideline identifies “best practices” for reporting security threats and incidents with the potential to significantly affect electricity infrastructure facilities or functions considered critical to the industry, as defined by each organization.

# Security Guidelines for the Electricity Sector: Threat and Incident Reporting

## Guideline Detail:

### The Need for Timely Reporting

All organizations should consider having in place processes to immediately report security threats and actual incidents that affect their operations and life safety to:

- law enforcement (e.g., local, state/provincial, FBI/RCMP);
- government agencies and regulators as is necessary or required (e.g., at the state/provincial or federal level);
- the Electricity Sector's Information Sharing and Analysis Center (ES-ISAC); and
- other electricity sector entities (e.g., control areas, reliability coordinators, regional transmission operators, independent system/market operators).

Some organizations are required by law to report threats or incidents within specified timeframes (e.g., DOE's Form EIA-417 Emergency Incident and Disturbance Report, NRC 10CFR73.71 and 10CFR73 Appendix G). All organizations are urged to understand these obligations and establish effective reporting processes.

Organizations should consider having in place threat and incident reporting processes that respond appropriately to the urgency of the situation. Reporting should be timely, based on the best available information, and promote the sharing of information on an actionable, need-to-know basis.

Organizations benefit from sharing threat and incident information in order to:

- promote a timely and actionable response in order to prevent the attack or mitigate the consequences on public health and safety, the environment and the economy;
- minimize negative impact on organization repair costs, revenues, productivity, customer service and public trust; and
- demonstrate diligence and due care by the organization on behalf of the electricity sector.

# Security Guidelines for the Electricity Sector: Threat and Incident Reporting

## Information to be Reported

The information to be reported will vary according to the specific circumstances and availability of the information, but should include:

- date, time and location of the incident
- brief description of incident
- impact on critical infrastructure, public health and safety, environment
- expected duration of impact, or time to restore
- cause, if known
- reporting individual and organization, and contact information for follow-up
- law enforcement involvement

## The Role of the ES-ISAC

The Electricity Sector – Information Sharing and Analysis Center (ES-ISAC) is operated by NERC and serves the electricity sector by facilitating communications between electricity sector organizations, the U.S. and Canadian federal governments and other critical infrastructure industries. The ES-ISAC promptly disseminates threat indications, analyses and warnings, together with interpretations, to assist electricity sector organizations to take protective actions.

The ES-ISAC facilitates communications and coordination with government agencies through the U.S. Department of Homeland Security<sup>2</sup> and Canada's Office of Critical Infrastructure Protection and Emergency Preparedness<sup>3</sup>.

## Information Confidentiality

If the information provided by an organization to the ES-ISAC is determined by the ES-ISAC to warrant an industry-wide warning, then any sensitive information would be sanitized and discussed with the organization providing the information before being disseminated.

---

<sup>2</sup> Ref. the FBI's National Infrastructure Protection Centre at [www.nipcc.gov](http://www.nipcc.gov) and the Department of Energy's Office of Energy Assurance at [www.oea.dis.anl.gov](http://www.oea.dis.anl.gov)

<sup>3</sup> Ref. [www.ocipep-bpiepc.gc.ca](http://www.ocipep-bpiepc.gc.ca)

# Security Guidelines for the Electricity Sector: Threat and Incident Reporting

Organizations providing incident information to government marked “Proprietary” or “Confidential” would be protected from public disclosure through exemptions from freedom of information legislation that provide for the protection of sensitive information concerning critical cyber or physical infrastructure, specifically:

- In the U.S., Freedom of Information Act exemption B4: Trade Secrets and Proprietary Information and Section 204 of the Homeland Security Act of 2002.
- In Canada, Sections 16(2)(c) and 20(1)(b) of the Access to Information Act.

## ES-ISAC Sharing of Information from Government Sources

The ES-ISAC receives sensitive-but-unclassified information from government intelligence and law enforcement sources and shares this with electricity sector organizations.

## Reporting Threats and Incidents

The ES-ISAC has collaborated with the FBI’s National Infrastructure Protection Center (NIPC) to develop a reporting process as described in the NIPC’s Standard Operating Procedure for their Indications, Analysis and Warning (IAW) Program. It is not essential that this specific reporting process and format be followed. For example, although electronic means are in place to facilitate reporting, telephone or fax are also acceptable reporting mechanisms. This procedure is available on the ES-ISAC web site and provides detailed instructions for reporting security threats or incidents, including:

- Responsibilities of participating organizations, the ES-ISAC and government
- Timeliness requirements
- Criteria and thresholds for reporting security **incidents** known or suspected to be of a malicious origin (eg. loss of >500 MW generation for 30 minutes or longer, loss of high-voltage substations or lines, loss of firm load >200 MW for longer than 30 minutes, anomalous or uncharacteristic market or power system operation)
- Criteria and thresholds for reporting security **threats** that potentially could affect the reliable operation of the electricity market or power system (e.g., surveillance activities, intrusion attempts, security breaches)

## **Security Guidelines for the Electricity Sector: Threat and Incident Reporting**

Three stages of reporting provide for different information requirements at each stage of the incident. An initial Stage 1 report is intended to provide early notice that an incident meeting one or more of the criteria and thresholds has occurred. Stage 1 reports are requested within the first 60 minutes after detection of an incident, with subsequent Stage 2 reports as conditions change. A final Stage 3 report is requested when the incident has been resolved or closed.

Organizations should consider several reporting mechanisms, including, but not limited to, the following:

1. The ES-ISAC's Critical Infrastructure Protection Information System (CIPIS) provides a secure Internet messaging system for communication with the ES-ISAC, the NIPC and ES-ISAC participants. CIPIS users must register and be authenticated by NERC as a valid participant. Registration can be initiated at:

<http://www.nerc.net/registration/>

2. NERC reliability coordinators are required to submit reports via the Reliability Coordinator Information System (RCIS).
3. Organizations should consider establishing reporting protocols with other electricity industry participants, critically interdependent customers or service providers, industry regulators, government and law enforcement organizations.

### **Exceptions:**

This security guideline does not pertain to communications and reporting procedures required for the real-time operation of the electricity markets and grid operations.

### **Related Documents:**

1. Electricity Sector Critical Infrastructure Protection Communications, prepared by NERC, dated July 5, 2002.
2. Indications, Analysis and Warning Program Standard Operating Procedure (IAW SOP) prepared by the FBI's National Infrastructure Protection Center, Rev 4.0, dated February 25, 2002.
3. NERC Security Guidelines for the Electricity Sector: Threat Response, Emergency Plans, Communications, Version 1.0, dated June 14, 2002.

# Security Guidelines for the Electricity Sector: Threat and Incident Reporting

## Revision History:

<b>Date</b>	<b>Version Number</b>	<b>Reason/Comments</b>
16 Jan 2003	Version - 0.8	Second draft as a result of Jan 16/03 CIPAG discussion

FR Doc 03-9126

[Federal Register: April 15, 2003 (Volume 68, Number 72)]

[Proposed Rules]

[Page 18523-18529]

From the Federal Register Online via GPO Access [wais.access.gpo.gov]

[DOCID:fr15ap03-44]

[[Page 18523]]

---

Part V

Department of Homeland Security

---

6 CFR Part 29

Procedures for Handling Critical Infrastructure Information; Proposed Rule

[[Page 18524]]

---

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 29

RIN 1601-AA14

Procedures for Handling Critical Infrastructure Information

AGENCY: Office of the Secretary, Homeland Security.

ACTION: Notice of proposed rulemaking.

---

SUMMARY: This notice of proposed rulemaking establishes for Federal  
Page 1

agencies the uniform procedures to implement Section 214 of the Homeland Security Act of 2002 regarding the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal Government. The protection of critical infrastructure reduces the vulnerability of the United States to acts of terrorism.

DATES: Written comments on this notice of proposed rulemaking may be submitted to the Department of Homeland Security on or before June 16, 2003.

ADDRESSES: Submit written comments (preferably an original and three copies) to Associate General Counsel (General Law), Department of Homeland Security, Washington, DC 20528. Electronic comments may be submitted to [cii.regcomments@DHS.gov](mailto:cii.regcomments@DHS.gov).  
FOR FURTHER INFORMATION CONTACT: Frank Nolan, (202) 282-8495, not a toll free call.

SUPPLEMENTARY INFORMATION:

I. Background

On November 25, 2002, the President signed into law the Homeland Security Act (Pub. L. 107-296), which created the new Department of Homeland Security (DHS) and established its responsibilities. Pursuant to the provisions of the Act, the Department came into existence on January 24, 2003.

The responsibilities of the Department include the taking of action to prevent terrorist attacks within the United States and to reduce the vulnerability of the United States to acts of terrorism. The reduction of that vulnerability includes the protection of vital physical or computer-based systems and assets, collectively referred to as "critical infrastructure," the incapacitation or destruction of which would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of these matters. The Department of Homeland Security recognizes the importance of receiving information from those with direct knowledge on the security of that critical infrastructure in order to reduce the vulnerability of this critical infrastructure to acts of terrorism.

The Department recognizes that its receipt of information pertaining to the security of critical infrastructure, much of which is not customarily within the public domain, is best encouraged through the assurance that such information will be utilized for securing the United States and will not be disseminated to the general public. Accordingly, section 214 of the Homeland Security Act, subtitle B of Title 2, which is referenced as the Critical Infrastructure Information Act of 2002 ("CII Act"), provides for the establishment of a critical infrastructure protection program that protects from disclosure to the general public any critical infrastructure information which the public may voluntarily provide to the Department.

Although the Homeland Security Act establishes a working definition of critical infrastructure information, the Department relies upon the discretion of the submitter as to whether the volunteered information meets the definition of critical infrastructure information. These procedures establish how critical infrastructure information volunteered by the public will be protected pursuant to section 214 of the Homeland Security Act.

## II. Notice of Proposed Rulemaking

This notice of proposed rulemaking establishes the procedures for protecting critical infrastructure information which are referenced in section 214(e) of the CII Act of 2002.

This regulation establishes uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily provided to the Federal Government by the public. These procedures apply to all Federal agencies that receive, care for, or store CII that is voluntarily submitted to the Federal Government pursuant to the CII Act of 2002. 6 U.S.C. 130, et seq. In addition, these procedures apply to United States Government contractors, to Foreign, State, and local governments, and to government authorities, pursuant to their express agreements.

## III. Procedural Requirements

In recognition of the importance of these procedures, the Department is providing this notice of proposed rulemaking of uniform procedures for the receipt, care, and storage of voluntarily submitted CII. As these procedures will affect Federal, State, and local governments and entities, the Department recognizes the importance of providing the opportunity for comment upon these procedures by both the government and private sector.

### Executive Order 12866

It has been determined that this rulemaking is a significant regulatory action for purposes of section 3(f)(4) of Executive Order 12866. This rulemaking is, however, not considered an economically significant regulatory action for the purposes of Executive Order 12866. This rulemaking has been reviewed and approved by the Office of Management and Budget.

### Regulatory Flexibility Act Certification

Because no notice of proposed rulemaking is required, the provisions of the Regulatory Flexibility Act (5 U.S.C. chapter 6) do not apply.

### Paperwork Reduction Act of 1995

OMB does not consider nonspecific or nondirective reporting--such as the information requested in the rule--that the respondent wishes to provide on a specific topic without further specification being sought to be subject to the Paperwork Reduction Act.

### List of Subjects in 6 CFR Part 29

Classified information, Confidential business information, Reporting and recordkeeping requirements.

### Authority and Issuance

For the reasons set forth above, 6 CFR is proposed to be amended by adding part 29 to read as follows:

PART 29--CRITICAL INFRASTRUCTURE INFORMATION

Sec.

- 29.1 Purpose and scope.
- 29.2 Definitions.
- 29.3 Effect of provisions.
- 29.4 Critical Infrastructure Information Program administration.
- 29.5 Authority to receive Critical Infrastructure Information.
- 29.6 Acknowledgment, validation, and marking of receipt.
- 29.7 Safeguarding of protected Critical Infrastructure Information.
- 29.8 Disclosure of information.
- 29.9 Investigation and reporting of violation of CII procedures.

Authority: Pub. L. 107-296, 116 Stat. 2135 (6 U.S.C. 1 et seq.);  
5 U.S.C. 301.

Sec. 29.1 Purpose and Scope.

(a) Purpose. This part implements Section 214 of Title II, subtitle B, of the Homeland Security Act of 2002 through the establishment of uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII)

[[Page 18525]]

voluntarily submitted to the Federal Government. Title II, subtitle B, of the Homeland Security Act is referred to herein as the CII Act of 2002. It is Department of Homeland Security (DHS) policy to encourage the voluntary submission of CII by protecting that information from unauthorized disclosure to the fullest extent permitted by law. As required by the CII Act of 2002, the procedures established herein include mechanisms regarding:

(1) The acknowledgement of receipt by a Federal agency of critical infrastructure information voluntarily submitted to the Federal Government;

(2) The maintenance of the identification of critical infrastructure information voluntarily submitted to the Federal Government for purposes of and subject to the provisions of the CII Act of 2002;

(3) The receipt, care, storage, and proper marking of the information as Protected CII;

(4) The protection and maintenance of the confidentiality of such information that permits the sharing of such information within the Federal Government and with Foreign, State, and local governments; and

(5) The issuance of notices and warnings related to the protection of critical infrastructure and protected systems in such a manner to protect from public disclosure the identity of the submitting person or entity, as well as information that is proprietary, business-sensitive, relates specifically to the submitting person or entity, and/or is not appropriately in the public domain.

(b) Scope. These procedures apply to all Federal agencies that receive, care for, or store CII voluntarily submitted to the Federal Government pursuant to the CII Act of 2002. In addition, these procedures apply to United States Government contractors, to Foreign, State, and local governments, and government authorities, pursuant to their express agreements.

Sec. 29.2 Definitions.

For purposes of this part:

(a) Critical Infrastructure has the same definition as described in section 2 of the Homeland Security Act of 2002, and means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof.

(b) Critical Infrastructure Information or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records or information concerning:

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety;

(2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(c) Critical Infrastructure Information Program or 'CII Program' means the maintenance, management, and review of these procedures and of the information provided to DHS in expectation of the protections provided by the CII Act of 2002.

(d) Information Sharing and Analysis Organization or ISAO means any 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 in order to better understand security problems and interdependencies related to critical infrastructure and protected systems to ensure the availability, integrity, and reliability thereof;

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

(3) Voluntarily disseminating critical infrastructure information to its members, Federal, State, and local governments, or any other entities that may be of assistance in carrying out the purposes specified in paragraphs (d)(1) and (d)(2) of this section.

(e) Local Government has the same meaning as established in section 2 of the Homeland Security Act of 2002, and means:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State

law), regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

(f) Protected Critical Infrastructure Information or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in Sec. 29.5 of this chapter. This information maintains its protected status unless the CII Program Manager renders a final decision that the information is not Protected CII.

(g) Protected System means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(h) Purpose has the meaning as described in section 214(a)(1) of the CII Act of 2002, and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.

(i) Submission to DHS as referenced in these procedures means any transmittal of CII from any entity to DHS. The CII may be provided to DHS either directly or indirectly via another Federal agency, which, upon receipt of the CII, will forward it to DHS.

(j) Voluntary or Voluntarily, when used in reference to any submission of

[[Page 18526]]

CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information; such submission may be accomplished by (i.e. come from) a single entity or an ISAO on behalf of itself or its members. The term does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings. In the case of any action brought under the securities laws--as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47)) the term "voluntary" does not include information or statements contained in any documents or materials filed, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 78l(i)) with the Securities and Exchange Commission or with Federal banking regulators; and with respect to the submission of CII, it does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities.

### Sec. 29.3 Effect of provisions.

(a) Freedom of Information Act access and mandatory submissions of

information. The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information that must be submitted to a Federal agency or pertaining to the obligation of any Federal agency to disclose such information under the Freedom of Information Act. Similarly, the CII Act of 2002 and these procedures do not apply to any information that is submitted to a Federal agency pursuant to any legal requirement. The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information or any other such information to a Federal agency under any other provision of law. Moreover, when information is required to be submitted to a Federal agency to satisfy a provision of law, it is not to be marked by the submitter, by DHS, or by any other party, as submitted or protected under the CII Act of 2002 or to be otherwise afforded the protections of the CII Act of 2002.

(b) Freedom of Information Act disclosure exemptions. Information that is separately exempt from disclosure under the Freedom of Information Act or applicable State or local law does not lose its separate exemption protection due to the applicability of these procedures or any failure to follow them.

(c) Restriction on use of protected CII by regulatory and other federal agencies. No Federal agency shall request, obtain, maintain, or use information protected under the CII Act of 2002 as a substitute for the exercise of its own legal authority to compel access to or submission of such information. Federal agencies shall not utilize CII for regulatory purposes without the written consent of the submitter.

(d) Independently obtained information. These procedures shall not be construed to limit or in any way affect the ability of a Federal, State, or local Government entity, agency, or authority, or any third party, under applicable law, to obtain information by means of a different law, regulation, rule, or other authority.

(e) No private rights or privileges. Nothing contained in these procedures is intended to confer any substantive or procedural right or privilege on any person or entity. Nothing in these procedures shall be construed to create a private right of action for enforcement of any provision of these procedures or a defense to noncompliance with any independently applicable legal obligation.

#### Sec. 29.4 Critical Infrastructure Information Program administration.

(a) IAIP Directorate Program Management. The Secretary of the Department of Homeland Security shall designate the Under Secretary of the Information Analysis Infrastructure Protection (IAIP) Directorate as the senior DHS official responsible for the direction and administration of the Critical Infrastructure Information Program.

(b) Appointment of CII Program Manager. The Under Secretary of IAIP shall:

- (1) Appoint a CII Program Manager within the IAIP Directorate to direct and administer the CII Program;
- (2) Commit necessary resources to the effective implementation of the CII Program; and
- (3) Promulgate implementing directives and prepare training materials as necessary for the proper treatment of Protected CII.

(c) Appointment of CII Officers. The CII Program Manager shall establish procedures to ensure that any DHS component or other entity that works with Protected CII appoints one or more employees to serve

as a CII Officer for the activity in order to provide proper management and oversight. Persons appointed to these positions shall be fully familiar with these procedures.

(d) Responsibilities of a CII Officer. The CII Officer shall:

(1) Oversee the storage and handling of Protected CII;

(2) Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the entity's storage, handling, and use of Protected CII;

(3) Establish additional procedures as necessary to prevent unauthorized access to Protected CII; and

(4) Ensure prompt and appropriate coordination with the CII Program Manager regarding any request, appeal, challenge, complaint, or suggestion arising out of the implementation of these procedures.

(e) Critical Infrastructure Information Management System (CIIMS). The CII Program Manager shall develop and use an electronic database, to be known as the "Critical Infrastructure Information Management System" (CIIMS), to record the receipt, acknowledgement, validation, storage, destruction, and disclosure of Protected CII. This compilation of CII shall be protected by the provisions of the CII Act of 2002.

#### Sec. 29.5 Authority to receive Critical Infrastructure Information.

(a) The Secretary of Homeland Security shall designate the DHS IAIP Directorate as the sole entity authorized to acknowledge and validate the receipt of Protected CII.

(b) CII shall receive the protections of section 214 of the CII Act of 2002 only when:

(1) Such information is voluntarily submitted either directly to the IAIP Directorate or indirectly to the DHS IAIP Directorate by submitting it to any Federal agency which then, pursuant to the submitter's express direction, forwards the information to the DHS IAIP Directorate;

(2) The information is submitted for use by DHS for the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purposes, as evidenced below, and

(3) The information is accompanied by an express statement as follows:

(i) In the case of written information or records, through a written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002"; or

(ii) In the case of oral information, within fifteen (15) calendar days of the

[[Page 18527]]

oral submission, through a written statement similar to the one above accompanied by a written or otherwise tangible version of the oral information initially provided.

(c) Information that is not submitted to the CII Program Manager, either directly by the submitter or indirectly through another Federal agency by request of the submitter, will not qualify for protection under the CII Act of 2002. Any Federal agency or DHS component, other

than the IAIP Directorate, that receives information with a request for protection under the CII Act of 2002 shall forward the information to the CII Program Manager. Only the CII Program Manager, or the Program Manager's designee, is authorized to acknowledge and validate the receipt of Protected CII.

(d)(1) Federal agencies, or DHS components other than the IAIP Directorate, shall maintain information as protected by the provisions of the CII Act of 2002 only:

(i) when that information is provided to the agency or component by the CII Program Manager, or his designee, and is marked ``Protected CII''; or

(ii) when the information is provided to the agency or component by the submitter pursuant to paragraph (b) of this section, that information is forwarded to the CII Program Manager pursuant to paragraph (c) of this section, and the CII Program Manager acknowledges and validates the information as ``Protected CII'' and authorizes the agency or component to mark the information as ``Protected CII''.

(2) The Federal agency or DHS component forwarding the information to the CII Program Manager may not disseminate, distribute, or make public the information until the CII Program Manager has notified the agency or component that the Program Manager has acknowledged and validated the information.

## Sec. 29.6 Acknowledgment, validation, and marking of receipt.

(a) Authorized official. Only the CII Program Manager, or the Program Manager's designee, is authorized to acknowledge and validate the receipt of information as Protected CII.

(b) Presumption of Protection. All information submitted in accordance with the procedures set forth herein will be presumed to be treated as Protected CII from the time the information is received by a Federal agency or DHS component. The information shall remain protected unless and until the CII Program Manager renders a final decision that the information is not Protected CII.

(c) Marking of information. In addition to markings made by submitters of CII pursuant to Sec. 29.5(b), all Protected CII shall be clearly identified through markings made by the CII Program Manager. The CII Program Manager shall mark CII materials as follows:  
``Protected Critical Infrastructure Information.''

(d) Acknowledgement of receipt of information. The CII Program Manager, or the Program Manager's designee, shall acknowledge receipt of information submitted as Protected CII, and in so doing shall:

(1) Contact the submitter, by the means specified in Sec. 29.7(e), within thirty (30) days of receipt;

(2) Maintain a database including date of receipt, name of submitter, description of information, and date and manner of acknowledgment; and

(1) At a minimum, provide the submitter with a unique tracking number whenever the information is provided to the CII Program Manager electronically by submission through an internet-enabled DHS on-line incident reporting form.

(e) Validation of information. (1) The CII Program Manager shall be responsible for reviewing all submissions that request protection under the CII Act of 2002. The Program Manager shall review the submitted information to validate the satisfaction of the definition of CII as established by law. In making this initial validation determination,

the Program Manager shall give deference to the submitter's expectation that the information qualifies for protection. However, if the Program Manager makes an initial determination that some or all of the information submitted does not meet the requirements for protection under the CII Act of 2002, the CII Program Manager shall:

(i) Notify the submitter of the initial determination that the information is not considered to be Protected CII. This notification also shall:

(A) Request that the submitter further explain the nature of the information and the submitter's basis for believing the information qualifies for protection under the CII Act of 2002;

(B) Advise the submitter that the CII Program Manager will review any further information provided before rendering a final determination;

(C) Notify the submitter that any response to the notification must be received by the CII Program Manager no later than thirty (30) days after the date of the notification; and

(D) Request the submitter to state whether, in the event the CII Program Manager makes a final determination that any such information is not Protected CII, the submitter prefers that the information be maintained without the protections of the CII Act of 2002 or be disposed of in accordance with the Federal Records Act.

(ii) If the CII Program Manager makes a final determination that the information is not Protected CII, the Program Manager, per the submitter's stated preference, shall either maintain the information without the protections of the CII Act of 2002 or dispose of it in accordance with the Federal Records Act. If the submitter, however, cannot be notified or the submitter's response is not received within thirty (30) days after the submitter received the notification, the Program Manager shall destroy the information in accordance with the Federal Records Act unless the Program Manager determines that there is a need to retain it for law enforcement and/or national security reasons.

(2) [Reserved]

(f) In the event the CII Program Manager determines that any information is not submitted in good faith accordance with the CII Act of 2002 and these procedures, the Program Manager is not required to notify the submitter that the information does not qualify as Protected CII. This is the only exception to the notice requirement of these procedures.

(g) Changing the status of CII to Non-CII. Only the CII Program Manager or the Program Manager's designee may change the status of Protected CII to non-Protected CII and remove its Protected CII markings.

## Sec. 29.7 Safeguarding of protected Critical Infrastructure Information.

(a) All persons granted access to Protected CII are responsible for safeguarding all such information in their possession or control. Protected CII shall be protected at all times either by appropriate storage or having it under the personal observation and control of a person authorized by the CII Officer to receive it. Each person who works with Protected CII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) Use and storage. During working hours, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized personnel. After working hours, Protected CII shall be stored in a secure container, such as a locked desk or file cabinet, or in a facility where Government or Government-contract security is provided.

(c) Reproduction. A document or material containing Protected CII may

[[Page 18528]]

be reproduced to the minimum extent necessary consistent with the need to carry out official duties, provided that the reproduced material is marked and protected in the same manner as the original material.

(d) Disposal of information. Material containing Protected CII shall be disposed of by any method that prevents unauthorized retrieval.

(e) Transmission of information. Protected CII shall be transmitted only by U.S. first class, express, certified, or registered mail, or through secure electronic means.

(f) Automated Information Systems that contain CII shall comply with the requirements of the Federal Information Security Management Act of 2002, 44 U.S.C. 3531-3538, implementing policy, and Office of Management and Budget Circular No. A-130, Appendix III.

## Sec. 29.8 Disclosure of information.

(a) Authorization of access. The Under Secretary of IAIP, or his or her designee, may choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority.

(b) Federal, State and Local Government access. The CII Program Manager may provide Protected CII to an employee of the Federal Government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose relating to homeland security. Protected CII may be made available to a State or local government entity only pursuant to its express agreement with the Program Manager that acknowledges the understanding and responsibilities of the recipient.

(c) Disclosure of information to Federal contractors. Disclosure of Protected CII to Federal contractors may be made after a CII Officer certifies that the contractor is performing services in support of the purposes of DHS. The contractor shall safeguard Protected CII in accordance with these procedures. Contractors shall not further disclose Protected CII to any of their components, employees, or other contractors (including subcontractors) without the prior written approval of a CII Officer unless such disclosure is expressly authorized in writing by the submitter.

(d) Further use or disclosure of information by State and Local governments. (1) State and local governments receiving information marked 'Protected Critical Infrastructure Information' shall not disclose that information to any other party, or remove any CII markings, without first obtaining authorization from the CII Program

Manager, who shall be responsible for requesting and obtaining written consent for any such State or local government disclosure from the person or entity that submitted the information.

(2) The CII Program Manager may not authorize State and local governments to further disclose or distribute the information to another party unless the Program Manager first obtains the written consent of the person or entity submitting the information.

(3) State and local governments may use Protected CII only for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.

(e) Disclosure of information to appropriate entities and the general public. The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the IAIP Directorate shall protect from disclosure the source of any voluntarily submitted CII that forms the basis for the warning; and any information that is proprietary, business-sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(f) Access by Congress and whistleblower protection. (1)(i) Pursuant to section 214(a)(1)(D) of the Homeland Security Act, Protected CII shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of the CII Act of 2002, except--

(A) In furtherance of an investigation or the prosecution of a criminal act; or

(B) when disclosure of the information is made--

(1) To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(2) To the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(ii) If any disclosure is made pursuant to these exceptions, prior written authorization must be obtained, in consultation with the DHS Office of the General Counsel, from the DHS Secretary, DHS Deputy Secretary, Under Secretary for IAIP, the DHS Inspector General, or the CII Program Manager.

(2) Consistent with the authority to disclose information for any purpose described in Sec. 29.2(h), disclosure of Protected CII may be made, without the written consent of the person or entity submitting such information, to the DHS Inspector General, or to any other employee designated by the Secretary of Homeland Security. Disclosure may be made by any officer or employee of the United States who reasonably believes that such information:

(i) Evidences an employee's or agency's conduct in violation of criminal law, or any other law, rule, or regulation, affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution; or

(ii) Evidences mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning,

interdependency study, recovery, or reconstitution.

(3) Disclosures of the above nature are authorized by law and therefore are not subject to penalty under section 214(f) of the Homeland Security Act of 2002.

(g) Responding to requests made under the Freedom of Information Act or State/local information access laws. (1) Protected CII shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the CII Program Manager, or the Program Manager's designee, to a State or local government agency, entity or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information. Any Federal, State, or local government agency with questions regarding the protection of Protected CII from public disclosure shall contact the CII Program Manager, who may in turn consult with the DHS Office of the General Counsel.

(2) These procedures do not limit or otherwise affect the ability of a State or local government entity, agency, or authority to obtain information directly from the same person or entity voluntarily submitting information to

[[Page 18529]]

DHS. Information independently obtained by a State or local government entity, agency, or authority is not subject to the CII Act of 2002's prohibition on making such information available pursuant to any State or local law requiring disclosure of records or information.

(h) Ex parte communications with decision-making officials. Pursuant to section 214(a)(1)(B) of the Homeland Security Act of 2002, Protected CII is not subject to `any agency rules or judicial doctrine regarding ex parte communications with a decision-making official.'

(i) Restriction on use of Critical Infrastructure Information in civil actions. Protected CII shall not, without the written consent of the person or entity submitting such information, be used by any Federal, State, or local authority, or by any third party, in any civil action arising under Federal or State law if such information is submitted in good faith for homeland security purposes.

(j) Disclosure to foreign governments. The CII Program Manager, or the Program Manager's designee, may provide Protected CII to a Foreign Government without the written consent of the person or entity submitting such information to the same extent it may provide advisories, alerts, and warnings to other governmental entities as described in Sec. 29.8(e) of this chapter, or in furtherance of an investigation or the prosecution of a criminal act.

(k) Obtaining written consent for further disclosure from the person or entity submitting information. Only the CII Program Manager, or the Program Manager's designee, may seek and obtain written consent from persons or entities submitting information when such consent is required under the CII Act of 2002 to permit disclosure. A person or entity's consent to additional disclosure, if conditioned both on a limited release of Protected CII for DHS's purposes and in a manner that offers reasonable protection against disclosure to the general public, shall not result in the information's loss of treatment as Protected CII.

Sec. 29.9 Investigation and reporting of violation of CII procedures.

(a) All persons authorized to have access to Protected CII shall report any possible violations of security procedures, the loss or misplacement of Protected CII, and any unauthorized disclosure of Protected CII immediately to the CII Program Manager, who shall in turn report the incident to the IAIP Directorate Security Officer and to the DHS Inspector General.

(b) Review and investigation of written report. The Inspector General, CII Program Manager, or IAIP Security Officer, shall investigate the incident and, in consultation with the Office of the General Counsel, determine whether a violation of procedures, loss of information, and/or unauthorized disclosure has occurred. If the investigation reveals any evidence of wrongdoing, DHS, through the Office of the General Counsel, shall immediately contact the Department of Justice, Criminal Division, for consideration of prosecution under the criminal penalty provisions of section 214(f) of the CII Act of 2002.

(c) Notification to originator of Protected CII. If the CII Program Manager or the IAIP Security Officer determines that an unauthorized disclosure occurred, or that Protected CII is missing, the CII Program Manager shall notify the submitter of the information in writing. The written notice shall contain a description of the incident and the date of disclosure, if known.

(d) Criminal and administrative penalties: Pursuant to section 214(f) of the Homeland Security Act of 2002, whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any CII protected from disclosure by the Homeland Security Act and coming to the officer or employee in the course of his or her employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under Title 18 of the United States Code, imprisoned not more than one (1) year, or both, and shall be removed from office or employment.

Dated: April 9, 2003.

Tom Ridge,  
Secretary of Homeland Security.  
[FR Doc. 03-9126 Filed 4-14-03; 8:45 am]

BILLING CODE 4410-10-P