



NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE (CIPC)

September 16, 2004 — 8 a.m.–5 p.m.
September 17, 2004 — 8 a.m.–12 p.m.

Hotel InterContinental New Orleans
444 St. Charles Avenue
New Orleans, Louisiana 70130
504-525-5566

AGENDA

- 15 minutes 1. **Administrative Items**
- Welcome and Introductions
 - Logistics: NERC Antitrust Compliance Guidelines, CIPC governance, proxies
 - Amend Agenda (**Approve**) — Stuart Brindley
 - June 9, 2004, CIPC Meeting Minutes (**Approve**) (reference material) — Lou Leffler
- 30 minutes 2. **NERC Update**
- Board of Trustees Retreat — Stuart Brindley
 - Operating and Planning Committees — Lou Leffler
 - Standards and Compliance Programs — Wally Johnson
- 45 minutes 3. **CIPC Executive Committee**
- CIPC Business Plan for 2005 — Stuart Brindley
 - Prioritization of Blackout Recommendations (reference material)
 - CIPC Action Items Review
 - Sector Coordinators
 - ISACCouncil — Lou Leffler
- 45 minutes 4. **ESISAC Subcommittee Updates**
- a. Outreach Working Group — Wally Johnson
Cyber Security Education Plan (**Approve**) (reference material to be forwarded) — Linda Nappier
 - 45 minutes b. Reporting Technologies Working Group — Carl Eng
 - Homeland Security Information Network (HSIN)
 - 15 minutes c. Indications, Analysis, Warnings Working Group — Larry Bugh

- 20 minutes d. ESISAC Performance During Hurricane Charley — Frank Prieto, Chuck Harper, Lou Leffler
- 10 minutes e. NESEC Task Force (now “National Electric Grid Monitoring System) — Jack Bernhardsen

5. Security Planning Subcommittee Updates

- 30 minutes a. Standards and Guidelines Working Group
 - Urgent Action Cyber Security Standard — 1200 — Larry Bugh
 - Permanent Cyber Security Standard — 1300
- 45 minutes b. Risk Assessment Working Group — Ted Heller
 - Critical Asset Definition (**Approve**) (reference material)
- 90 minutes c. Process Control Systems Security Task Force
 - Security Guideline: Physical Security — Substations (**Approve**) (reference material) — Tom Flowers
 - Security Guideline: Secure Connectivity of Control Systems (for awareness and future action) — Elizabeth Rhodenizer
 - Security Guideline: Cyber Patch Management (reference material) — Linda Nappier
 - Comments on DOE document “21 Steps to improve Cyber Security of Control System Networks” (**Approve**) (reference material) — Linda Nappier
 - Top Ten Vulnerabilities of Control Systems (reference material) — Scott Mix
- 10 minutes d. Public Key Infrastructure Task Force — Larry Bugh
- 30 minutes e. Critical Spares Task Force — Michael Innocenzo

6. Agency Briefings (as available)

- 20 minutes a. Public Safety and Emergency Preparedness Canada — Kara Yorke
- 20 minutes b. Department of Energy — Alex DeAlvarez (invited)
 - National Infrastructure Protection Plan — Hank Kenchington
- 20 minutes c. Department of Homeland Security — Paul Carrier
 - Interagency Security Plan
- 20 minutes d. Federal Energy Regulatory Commission — Cynthia Pointer, Bruce Poole (invited)

60 minutes **7. Follow-up and Actions From All Briefings and Working Group/task force Reports — All**

8. Other — All

- 10 minutes **9. Future Meetings (approve) — Lou Leffler**
 - a. November 11–12, 2004, Kansas City, Missouri (coupled with NERC standing committees)
 - b. March 17–18, 2005, Long Beach, California (coupled with NERC standing committees)

- c. June 2005, Washington, D.C. (possibly coupled with DHS cleared briefing)
- d. September 15–16, 2005, Philadelphia, Pennsylvania (coupled with AGA, EEI, NERC standing committees)
- e. December 8–9, 2005, St. Petersburg, Florida (coupled with NERC standing committees)
- f. Security briefing conference calls will be conducted on the first and third Fridays each month and as conditions require
- g. CIPC, working group, task force conference calls will be conducted as required

Background Materials

1. Minutes of the June 9, 2004 NERC CIPAG Meeting, Draft 2
2. Joint Task Force Outage Recommendations and CIPC Response
3. Cyber Security Education Plans (to be forwarded)
4. Critical Asset Definition
5. Security Guideline: Physical Security — Substations
6. Security Guideline: Cyber Patch Management
7. Comments and Suggestions for Consideration by the Department of Energy in Issuing a Second Release of the “21 Steps to Improve Cyber Security of SCADA Networks”
8. Top Ten Vulnerabilities of Control Systems
9. Organization and Procedures Manual for NERC Standing Committees
< ftp://www.nerc.com/pub/sys/all_updl/docs/misc/orgproman061003.pdf >
10. Other Materials to be Forwarded as Available



North American Electric Reliability Council

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

CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE (CIPC) MEETING MINUTES

June 09, 2004
Washington, DC

Draft-2

This meeting's agenda was announced via email dated 21 May 2004. A quorum was present for all business. The NERC Antitrust Guidelines were read. Member proxies were announced.

Attendees

Refer to attachment to these minutes. Formal proxies are noted thereon.

Presentations and Documents

The following materials are posted on the CIPC open or private files section of the NERC Internet site:
File CIPC Confidentiality definitions:

1. Public Release: Publicly available (posting on open CIPC Internet site).
2. Electricity Sector Only: Available to CIPC Members, Alternates, and Associates for their use including distribution at their discretion to NERC Regions and Electricity Sector Associations but with no further distribution (posting on CIPC Internet private files site).
3. CIPC Only: Available to CIPC Members, Alternates, and Associates for their use but with no further distribution (posting on CIPC Internet private files site).
4. No Distribution: No further availability (will not be posted).

Topic	Presenter	Availability
CIPC Executive Committee Update: June 09, 2004	Stuart Brindley	Public Release
Critical Spares Task Force Report	Ken Hall, Bipin Patel, Ron Niebo	Electricity Sector Only
Critical Infrastructure Protection: International Information Exchange for the Electricity Sector	Larry Brown, John Allen	Public Release

Future Meetings

1. Thursday (0800-1700 hr) – Friday (0800-1200 hr), 16-17 September 2004; New Orleans (coupled with EEI Security Committee).
2. Thursday (0800-1700 hr) – Friday (0800-1200 hr), 11-12 November 2004; Kansas City, MO (coupled with NERC Standing Committees).
3. Thursday (0800-1700 hr) – Friday (0800-1200 hr), 17-18 March 2005; San Diego (coupled with NERC Standing Committees).
4. (Date to be determined) early June 2005; DC (possibly coupled with DHS cleared briefing).
5. Thursday (0800-1700 hr) – Friday (0800-1200 hr), 15-16 September 2005; Philadelphia, PA (coupled with AGA, EEI, NERC Standing Committees).
6. Thursday (0800-1700 hr) – Friday (0800-1200 hr); 08-09 December 2005; Tampa, FL (coupled with NERC Standing Committees).

7. Security briefing conference calls will be conducted on first and third Fridays each month and as conditions require.
8. Activity conference calls will be conducted as required.

Actions by Motion

The following actions were taken at this meeting and approved by motions:

Motion 1: Moved: Bob Beahm; Seconded; Action: Passed, no dissenting votes.
Approve Minutes of the March 25-26, 2004 meeting, draft-2 as submitted.

Motion 2: Moved: Jack Bernhardsen; Seconded; Action: Passed, no dissenting votes.
Approve agenda for this meeting of the CIPC, draft-3.

Motion 3: Moved: Eric Solberg; Seconded; Action: Passed, no dissenting votes.
Accept the verbiage regarding the availability of CIPC files as stated under "Presentations and Documents" herein. In addition, an abbreviated notation will be included on all pages. Materials will be posted in pdf.

Motion 4: Moved: Jack Bernhardsen; Seconded; Action: Passed, no dissenting votes.
Accept the Critical Spares Task Force Work Plan.

Motion 5: Moved: Bob Canada; Seconded; Action: Passed, no dissenting votes.
Accept the Risk Assessment Working Group Work Plan.

Motion 6: Moved: Larry Dolci; Seconded; Action: Passed, no dissenting votes.
Accept the Indications, Analysis, Warnings Working Group Work Plan.

Motion 7: Moved: Control Systems Security Working Group; Action: Passed: 1 no, 2 abstentions.
CIPC accepts the Security Guideline: Time Stamping of Operational Data Logs to forward to the NERC Operating and Planning Committees for acceptance to send to the NERC Board for approval.

Follow-Up Actions

Refer to CIPC Action Items, 09 June 2004, made part of these minutes.

1. The CIPC Executive Committee will manage the Action Items list regarding completions and assignments.
2. CIPC EC to prioritize the Joint US-Canada Outage Task Force Recommendations in consultation with the Security Working Group of the US-Canada Outage Task Force.
3. Consider a Critical Spares awareness program.
4. Request Operating Committee personnel support to the Critical Spares Task Force.
5. Lou Leffler will request information from the George Mason University CIP Program regarding work they are doing regarding categorization of risk assessment methodologies.
6. CIPC Executive Committee will provide guidance to a CIPC role in an expanded international "bi-lateral" collaboration on CIP.
7. Linda Nappier will chair a group (and will coordinate with the Outreach WG) to provide support information to the ES regarding Cyber Security Standard compliance.
8. Comments to the DOE on "21 Steps to Improve Cyber Security of Control System Networks" will be forwarded by NERC to DOE.
9. Forward Security Guideline: Time Stamping of Operational Data Logs to the Operating and Planning Committees for acceptance to send to the NERC Board for approval.
10. CIPC and CIP Forum should comment to Tom Flowers on the draft Security Guideline: Physical Security – Substations.

11. Send comments and support ideas on the draft Security Guideline: Secure Connectivity of Control Systems to Elizabeth Rhodenizer.
12. Set up listserv for the Control Systems Connectivity group.
13. Pursue possible use of cyber and physical security personnel on NERC readiness audits.
14. Mike Peters will distribute the revised documents to CIPC, via NERC: "Information Threat Handbook", "Terrorist Threat Handbook", "OPSEC Basics".

(Numbers following topic are those in the meeting Agenda.)

NERC Report (2)

Work on Version-0 of the NERC Standards has commenced.

August 14, 2003 Outage Recommendations (3)

The Joint Canada-US Task Force on the Outage report contains 46 recommendations to help prevent and mitigate a future outage of the kind experienced on 14 August 2003. Twenty of the recommendations may require either significant or minimal input by CIPC. The CIPC Executive Committee will provide leadership in assuring CIPC contribution as required. Some input will be sought from the US-Canada Joint Task Force. The recommendations will be reviewed, prioritized, and assigned to CIPC working groups and task forces as appropriate. NERC is maintaining a recommendations database that is to be updated weekly.

Alison Silverstein noted that the Federal Energy Regulatory Commission (FERC) is treating the recommendations as good utility practice. The FERC is considering treatment in rates regarding the costs to meet recommendations.

CIPC Executive Committee Report (5)

(Refer to presentation.)

Stuart Brindley reported for the Executive Committee.

The Executive Committee accepted the proposed name change of the Process Control Systems Security Task Force to Control Systems Security Working Group to provide a more accurate name for the work plan and to recognize the longer term nature of this work. The Executive Committee combined two of the ESISAC WGs (Indications, Analysis, Warnings WG and Analysis WG) into a single IAW WG, led by Larry Bugh.

Sector Coordinators (5)

Stuart Brindley reported on recent activities of the Sector Coordinators including the recent meeting in May 2004. Stuart, as CIPC Chair, will represent the Electricity Sector with the Sector Coordinators at meetings and conference calls.

Information Sharing and Analysis Council (5)

Lou Leffler reported on the recent activities of the ISAC Council. There are currently twelve ISACs engaged in the development of inter-ISAC practices including communications (information to share and mechanisms). The necessity to provide an all-threats capability among the ISACs is stressed by the Council; this refers to situational information sharing and analysis for intentional, accidental, and natural events, threats, and vulnerabilities.

The white papers created by the Council over the last year are now available at:
<http://www.isaccouncil.org>

A Matrix of activities and contacts is under development with input from each ISAC to describe its posture in several common areas of concern.

Risk Assessment Working Group (6b)

Ted Heller reported for the Working Group.

One task is the development of a risk assessment methodology/tool "catalog". This may be a list of available tools by name or perhaps a list of desired characteristics to be included in a risk assessment approach. It was noted that no one tool meets all ES needs. The DHS may be planning to perform a risk assessment tool evaluation. It was reported that George Mason University through its CIP Program may be doing work in this area; this will be pursued.

Consideration should be given to natural gas facilities that could be defined as critical to critical ES facilities.

As reported by Bob Windus, BPA developed a set of criteria for use in determining its most critical facilities. The criteria helped to establish the rank order of facilities for application of the RAM-T risk assessment evaluation. The criteria used are:

- Economic Security
- National Security
- Regional and North American Grid Security
- Public Health and Safety
- Generation (Substation)

This BPA criterion was provided to the General Accounting Office during a recent GAO Survey of CIP activity within the ES.

The revised Risk Assessment Working Group Work Plan was discussed and approved; refer to Motion-5.

Reporting Technologies Working Group (7b)

Representatives from the DHS presented on the Homeland Security Information System HSIN. The ES was requested by DHS in May to be a trial user of HSIN via the ESISAC, initially. This was approved by the CIPC Executive Committee. The currently operational US-CERT Portal will be included in HSIN. DOE, as Sector Specific Agency in HSPD-7 for Energy, will be invited to participate in HSIN. The RISS ATIX program may be integrated with HSIN. HSIN is expected to be the official tool for communications regarding terrorism. DHS was urged to assure ultimate development of a coordinated system for communications. The CIPIS may be incorporated into HSIN.

Additional information on the National Cyber Security Partnership is available at:
<http://www.cyberpartnership.org>

Indications, Analysis, Warnings (IAW) Working Group (7c)

Larry Bugh reported for the Working Group.

The IAW WG now incorporates the former Analysis Working Group. A revised IAW WG Work Plan was approved; refer to Motion-6.

Cyber Security Standard (6a)

Larry Bugh discussed the 1200 and 1300 Cyber Security Standards.

The Urgent Action 1200 Standard has a one year life that ends August 2004 unless extended for a one more (maximum) year. The compliance for 2005 is expected to be 100% for those entities identified in the implementation plan (with reporting by the Reliability Coordinators and Control Areas). The ballot body registration is now open. The voting will commence 02 July 2004 for a ten day period. The Implementation plan spells out the compliance requirements. There is concern regarding to what

entities the extended 1200 will apply; it is the same for 2005 as was the case for 2004. This should be clarified to the Electricity Sector.

The Regions have completed the summary for the 2004 compliance "snapshot". The CIPC Cyber representatives have met (conference calls) to find ways to help the ES to achieve the goal of making compliance 100% for reporting entities by 2005. Ideas were presented as captured in a report: "Proposal To Reach Full Compliance With Cyber Security Standard 1200" (distributed to CIPC by email on 02 June 2004). Some Regions expect to be fully compliant. A workshop or other form of communication may be helpful to other Regions and to all Regions in preparing for the 1300 Standard. Even though only Reliability Coordinators and Control Areas must submit compliance reports during the application of the 1200 Standard, all entity types (in accordance with the NERC Functional Model) as defined in each of the 16 Standards should become compliant. The following comments were made:

1. Consider what proportion of entities indicate they plan to be compliant by 2005.
2. Do workshops or web casts as the presentation medium.
3. Stress the requirements and to whom they apply.
4. Focus on the ready access to support information.
5. Make presentations to those Regions so desiring and at their convenience.
6. Affirm the target audiences.
7. Clarify the meaning of "compliance".

Linda Nappier will chair a small group and will coordinate with the Outreach WG to define the approach. There was general consensus to move ahead; it was noted that NERC Management strongly supports this effort.

The 1300 Permanent Cyber Security Standard work has commenced. The Standards Authorization Committee (SAC) has approved the Standard Authorization Request (SAR). SAC has approved the SAR Drafting Team with others who self nominate and are accepted by the SAC to constitute the Standard Drafting team. Definition of Critical Assets as being developed by the Risk Assessment WG will be considered. The current goal is to get first draft of 1300 out for comment in August 2004. Expansion of scope to other entities and inclusion of control systems is a major change and issue; goes to the critical facilities definition. Another significant issue is background screening.

Security Guides and Standards Working Group (6a)

John Maguire reported for the Working Group.

There has been some review of the Time Stamping Guideline, the Vulnerability and Risk Assessment Guideline, the Physical Security of Unstaffed Facilities Guideline, Secure Connectivity of Control Systems Guideline. The Threat Alert System and Response Guidelines will be presented for CIP Forum review. A security guideline on IT system patching is under consideration. The WG is also working on definition of critical facilities. John will draft a description of the process for development and review of new and revised guidelines; guideline content is developed by other WGs and TFs; the Security Guides and Standards WG stands to assist in the overall process, and documentation of this process. The WG had major input to the NERC response to the PCII rulemaking.

Critical Spares Task Force (6e)

(Refer to presentation.)

Bipin Patel, Consultant to NERC and facilitator of the Critical Spares Task Force was introduced to CIPC.

Bipin, Ken Hall, and Ron Niebo presented for the Task Force.

The spare transformer database is growing and was successfully dry run tested. However, not all spare transformers are included. The database must be updated as changes occur. It was noted that even though a spare exists and is included in the database, the owner may not be able to make it

available if needed by another entity. The DOE is exploring application of the Defense Production Act to help assure the availability of critical spares.

The task force is considering expanding the database to other critical bulk electric system components. CIPC cautioned that it would be most useful to get the transformer spares program solidified, then consider expansion to other equipment.

The critical spares work is part of risk management; the NERC Operating Committee should have the opportunity for input, at least certain awareness of this capability. The OC will be asked to provide support personnel to the Task Force.

The means to participate in the program and the availability of information included therein must be explained to the ES through an awareness program.

The FERC transformer study is expected to be complete in July 2004.

There are many issues including the consideration of a spares pool, with funding. Consider expanding the database to include transformers with high side voltage less than 345 kV and generator step up transformers. DHS is working on a recovery transformer. It is suggested that the Critical Spares Task Force be the primary point of contact as the projects progress.

The DHS Buffer Zone Protection (BZP) program was discussed. Critical sites for any infrastructure as determined by DHS (suggested, in consultation with the ES) will receive protection. BZP is performed in conjunction with the States and Local Law Enforcement. The buffer zone is essentially outside the critical facility. Owner/operators can request consideration be given to inclusion of their critical facilities.

The Critical Spares TF Work Plan was presented, discussed, and approved; refer to Motion-4.

Control Systems Security (CSS) Working Group (6c)

Scott Mix reported for the Working Group.

The WG prepared comments to the DOE Document: "21 Steps to Improve Cyber Security of Control System Networks". The DOE document was developed in 2002, and the WG believes that its comments would be useful for consideration to a document update. These comments (together with the individual discussions, without attribution) will be sent to the DOE via NERC. Linda Nappier is the CIPC point of contact.

The proposed Security Guideline: Time Stamping of Operational Data Logs was discussed. This guideline addresses a Recommendation-28 in the Joint US-Canada Outage Task Force Report. The guideline was initiated by the CSSWG to deal with the technical aspects of time stamping, not the specific data nor locations thereof. The guideline will be forwarded to the Operating and Planning Committees for acceptance to send to the NERC Board for approval; refer to Motion-7.

Tom Flowers presented the draft Security Guideline: Physical Security – Substations. This is a very important concept and will be presented for further consideration by the Control Systems Security and Standards and Guidelines Working Groups. No action was requested at this meeting. Comments should be submitted to Tom Flowers.

Elizabeth Rhodenizer presented the draft Security Guideline: Secure Connectivity of Control Systems. This guideline is generated from the most critical aspects of the DOE Document: "21 Steps to Improve Cyber Security of Control System Networks", those aspects that are not already covered by existing

Security Guidelines or the Cyber Security Standard. Existing control system operational policies, comments, and support should be sent to Elizabeth.

National Electric Infrastructure SECURITY (NESEC) System Task Force (7d)

Jack Bernhardsen reported for the Task Force.

No progress can be reported on either the manual or the automated program. The Reliability Coordinators believe this to be a valuable program for their own use and for the Department of Homeland Security (DHS).

Public Key Infrastructure (PKI) Task Force (6d)

Larry Bugh reported for the Task Force.

Work continues on this project. Further review of the original approach is being conducted.

Cyber Intrusion Detection System Pilot Project Task Force (7e)

Stuart Brindley reported for the Task Force.

The project is underway among participating Independent System Operators for initial implementation, Fall 2004.

DHS Protected Critical Infrastructure Information (8c)

(Presentation package distributed in hard copy.)

Fred Herr, Director of PCII Office at DHS presented the status of the program. The PCII Office has responsibility to assure the handling and protection of voluntarily submitted information. The Office is considering a blanket authorization to submit PCII to the NICC without the PCII Office being in the path. Currently submissions must be in hard form (i.e. written, fax, tape, disc); must be signed. Working on means to receive and properly disseminate electronically. For protection, any reporting entity will need to make arrangements with the PCII Office; possibility for an ISAC to send on behalf of other entities; needs clarification. Submitted PCII comments, by NERC and others, will be considered. Larry Brown will work with NERC General Counsel on creating a pre-approved reporting mechanism for the IAW program. The program will not be ready for extension to the states for a year. An accreditation program will be established by DHS to assure that disseminated information is handled properly; this includes training. Send questions to: pcii-info@dhs.gov
Additional information available at: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0404.xml

Federal Energy Regulatory Commission (FERC) (8d)

Alison Silverstein reported for the FERC.

The FERC is performing a study on the number and types of transformers in use on the bulk electric system and are doing equipment pool scoping.

The FERC's Critical Energy Infrastructure Information (CEII) program is in place and no issues have been identified to date.

It was suggested that consideration be given to including physical security experts as part of the NERC readiness audit teams. CIPC may consider requesting some anonymized input/observations from the teams regarding security. Seek if there is a readiness document used by the teams that can be shared with CIPC.

Four gas pipeline disruption studies have been conducted; four more geographic areas to be conducted. These studies will lead to interdependency analyses.

A security cost recovery document is being developed by FERC and will be made available. FERC will conduct a workshop, 14 July 2004, on cyber security of control systems.

Alison was thanked for her contributions to the CIPC and the ES.

Department of Public Safety and Emergency Preparedness (PSEPC) (8a)

Elizabeth Rhodenizer presented for the PSEPC.

PSEPC is investigating the benefit to developing a "need for security" document. The resulting product from this initiative will be distributed through the CIPC.

Department of Energy Office of Energy Assurance (DOE-OEA) and R&D (8b)

Hank Kenchington presented for the DOE-OEA.

The National Infrastructure Protection Plan (NIPP) is under development for the Energy Sectors by the DOE as called for in HSPD-7. The first draft of the NIPP is expected to be transmitted to the DHS in June and to the ISACs in July. Completion of the initial plan is scheduled for the latter part of 2004. It is understood that this plan will be an ongoing project.

Interagency Security Plan (ISP) (8b)

Jim McGlone discussed the development of the ISP.

The plan will be presented, by DHS, to the President of the United States this week. There was some interaction with the DOE-OEA and the ES (Risk Assessment WG and Control Systems Security WG). Questions remain regarding the protection of named (in the report) critical assets. The asset lists had been assembled by DOE with limited review by the ES.

Two concerns were expressed by CIPC:

- To be most effective the development of specific plans must be done collaboratively by the governments (federal, state, local, tribal) and critical infrastructure owners and operators.
- It is essential that the ES remain aware of future challenges to stay in front as much as possible, while also recognizing the limited number of knowledgeable people to do this critical work.

Infrastructure Coordination Division (ICD), Department of Homeland Security (DHS) (8c)

Paul Carrier discussed the process for obtaining US Government security clearances by ES personnel.

Most of the pre-existing clearances were held by the DOE; these have been (or are being) transferred to DHS. There are some special cases (clearances held by other agencies); holders should contact Paul for details. Earlier this year a request for those interested in pursuing clearances was sent by the DHS. Of those requests received, eight are currently in process and individuals will be contacted by DHS.

Critical Infrastructure Protection: International Information Exchange; Electricity Sector (9)

(Refer to presentation.)

Larry Brown and John Allen, LogOn/ESAA, reported on the Fourth US-Australian bilateral discussions on critical infrastructure protection.

Each of the involved countries can learn from work done in areas such as standards, exercises, control systems. The next government-sponsored bi-lateral conference for all critical industry sectors will be conducted in the United States, April 2005. John is working with the Australian government and electric sector to implement an electric-only bilateral program (and this effort is expected to include Canada). The first exploratory meeting for such an effort is expected to be this Fall in Australia. The CIPC Executive Committee will take an action item to move this forward within the CIPC, with focus on the presentation slide: Potential NERC Participation.

CIPAG Meeting Attendees

09 June 2004

(P=Proxy)

REPR	VOTE	POSITION	NAME	ORGANIZATION
APPA	V	Member	Sandy Brewer	Conway Corp
	P	Alternate	James Strange	APPA
CEA	V	Member Chair Exec Cmte	Stuart Brindley	IMO
NRECA	V	Member	Bob Richhart	Hoosier Energy
	V	Member	Barry Lawson	NRECA
ECAR	V	Member: Phys	Michael Lynch	Detroit Edison
	V	Member: Cybr Vice Chair Exec Cmte	Larry Bugh	ECAR
	V	Member: Oper	Scott Moore	AEP
		Alternate: Cyber	Jerry Freese	AEP
ERCOT	V	Member: Phys	Bill Bojorquez	ERCOT
	P	Member: Oper	John Adams	ERCOT
FRCC	V	Member: Cybr	Brian Malfant	FRCC
MAAC	V	Member: Phys	Robert H. Beahm	BGE
	V	Member: Cybr	John Maguire	PJM
		Alternate: Phys	Ed Stowe	PEPCO
MAIN	V	Member: Phys Vice Chair Exec Cmte	Pat Laird	Exelon
	V	Member: Oper	Eric Solberg	ATC
	V	Member: Cybr	Linda Nappier	Ameren Services
		Alternate: Cybr	Kurt Muehlbauer	Exelon
		Alternate: Oper	Rich Gloff	MAIN
MAPP	V	Member: Cybr	Greg Fraser	Manitoba Hydro
NPCC	V	Member: Cybr	Chuck Noble	ISO New England
	V	Member: Phys	Ronald P. Belval	Vermont Elec Pwr
		Member: Oper	Roger Lampila	New York ISO
		Alternate: Phys	Bruce Metruck	New York PA
		Alternate: Cybr	Brian Hogue	NPCC
SERC	V	Member: Phys Exec Cmte	Bob Canada	Southern
	V	Member: Cybr	Jay Cribb	Southern
	P	Alternate: Cybr	Dave Norton	Entergy
		Alternate: Oper	Russell Robertson	TVA
SPP	V	Member: Cybr	Todd Thompson	SPP
	V	Member: Oper	Allen Klassen	Westar Energy
	V	Member: Phys	Larry Dolci	Great Plains Energy
WECC	V	Member: Cybr Exec Cmte	James Sample	Cal ISO
	V	Member: Phys	Bob Windus	BPA
		Alternate: Phys	Lyman H. Shaffer	Pacific G&E
	P	Alternate: Oper	Jack Bernhardsen	PNSC

NERC		Secretary Exec Cmte	Lou Leffler	NERC
		Staff Support	Lyn Costantini	NERC
		Staff Support	Ron Niebo	NERC
		Staff Support	Bipin Patel	NERC
-----		Associate	Joe Bucciero	KEMA
		Associate	Hein Gerber	CEA
		Associate	Brian Bell	DHS-CSC
		Associate	Mike Ferrara	DHS-CSC
		Associate	Julie Silberger	DHS-CSC
		Associate	Paul Carrier	DHS-MITRE
		Associate	Michael Cohen	DHS-MITRE
		Associate	Mike Peters	DOD
		Associate	Jim McGlone	DOE-OEA
		Associate	Mark Engels	Dominion Resources
		Associate	Ted Heller	DPO-MA
		Associate	Mike Knauer	Hoosier Energy
		Associate	Larry Brown	EEI
		Associate	Ken Hall	EEI
		Associate	Scott Mix	EPRI
		Associate	Bruce Poole	FERC
		Associate	Alison Silverstein	FERC
		Associate	Chris Shepherd	ICCT
		Associate	John Allen	Logon Consulting
		Associate	Jason Remer	NEI
		Associate	Matthew Chiramal	NRC
		Associate	Eric Lee	NRC
		Associate	Patrick Tronnier	OATI
		Associate	Tom Iwanski	PRPA
		Associate	Michael Regan	PSEG
		Associate	Elizabeth Rhodenizer	PSEPC
		Associate	John Pavek	RUS
		Associate	Chris Decker	SMEPA

**AUGUST 14, 2003 OUTAGE RECOMMENDATIONS
US-CANADA TASK FORCE**

CONFIDENTIAL

Priority for CIPC
H = High
M = Medium
L = Low
N = Not
C = Complete (CIPC part)

**FOCUS
NERC CRITICAL INFRASTRUCTURE PROTECTION COMMITTEE**

**Not for further
distribution**

* leading Recommendation # = Updated response

Pr	Recommendation Description	Summary	CIPC Response
L	4. Clarify that prudent expenditures and investments for bulk system reliability (including investments in new technologies) will be recoverable through transmission rates.	Clarify that prudent expenditures and investments by regulated companies to maintain or improve bulk system reliability will be recoverable through transmission rates. Identify and resolve issues related to the recovery of reliability costs and investments through retail rates.	Applies to physical and cyber security measures. Maintain awareness of this issue and the work being done in the US by the National Association of Regulatory Utility Commissioners (NARUC). CIPC Executive Committee
M	5. Track implementation of recommended actions to improve reliability.	A. NERC should establish mechanisms for tracking and reporting to the public on implementation actions in their respective areas of responsibility. B. NERC should prepare annual reports to FERC, appropriate authorities in Canada, and the public on the status of the industry's compliance with recommendations and important trends in electric system reliability performance.	Update responses to recommendations assigned to the CIPC. CIPC EC
C	11. Establish requirements for collection and reporting of data needed for post-blackout analyses.	FERC and appropriate authorities in Canada should require generators, transmission owners, and other relevant entities to collect and report data that may be needed for analysis of blackouts and other grid-related disturbances.	Security Guideline: Timestamping of Operational Data Logs has been drafted and approved by CIPC at its June 2004 meeting. This SG contains the technical details. Other NERC committees will determine data to which timestamping applies and the precision required. The SG will be sent to the OC and PC.

Pr	Recommendation Description	Summary	CIPC Response
H	20. Establish clear definitions for normal, alert and emergency operational system conditions. Clarify roles, responsibilities, and authorities of reliability coordinators and control areas under each condition.	NERC should develop by June 30, 2004 definitions for normal, alert, and emergency system conditions, and clarify reliability coordinator and control area functions, responsibilities, required capabilities, and required authorities under each operational system condition.	Control Systems Security WG Support to Operating Committee, with respect to reporting including participating in the proposed North American Electric Infrastructure Security Monitoring System (NESEC) project. The Homeland Security Information Network (HSIN) may significantly help communications among Reliability Coordinators and possibly Control Areas. Reporting Technologies WG NESEC TF
H	26. Tighten communications protocols, especially for communications during alerts and emergencies. Upgrade communication system hardware where appropriate.	NERC should work with reliability coordinators and control area operators to improve the effectiveness of internal and external communications during alerts, emergencies, or other critical situations, and ensure that all key parties, including state and local officials, receive timely and accurate information. NERC should task the regional councils to work together to develop communications protocols by December 31, 2004, and to assess and report on the adequacy of emergency communications systems within their regions against the protocols by that date.	Enhance the capabilities of the ESISAC to communicate security threats and incidents. Consider including situational awareness with the duties. HSIN may significantly help as might additional reliable communication techniques. Reporting Technologies WG ESISAC SC
C	28. Require use of time-synchronized data recorders.	A. FERC and appropriate authorities in Canada should require the use of data recorders synchronized by signals from the Global Positioning System (GPS) on all categories of facilities whose data may be needed to investigate future system disturbances, outages, or blackouts. B. NERC, reliability coordinators, control areas, and transmission owners should determine where high-speed power system disturbance recorders are needed on the system, and ensure that they are installed by	A new Security Guideline: Timestamping of Operational Data Logs has been approved by CIPC for transmittal to the NERC PC and OC. Refer to Rec-11. Control Systems Security WG Other NERC Committees

Pr	Recommendation Description	Summary	CIPC Response
		<p>December 31, 2004.</p> <p>C. NERC should establish data recording protocols.</p> <p>D. FERC and appropriate authorities in Canada should ensure that the investments called for in this recommendation will be recoverable through transmission rates.</p>	
H	30. Clarify criteria for identification of operationally critical facilities, and improve dissemination of updated information on unplanned outages.	NERC should work with the control areas and reliability coordinators to clarify the criteria for identifying critical facilities whose operational status can affect the reliability of neighboring areas, and to improve mechanisms for sharing information about unplanned outages of such facilities in near real-time.	<p>CIPC will work with other NERC Committees and the Governments in this very sensitive area. The Risk Assessment WG will develop a concise definition of critical assets and with governments determine use and protection of any lists of such assets. Critical assets should be determined with a view towards both electric grid and load considerations. The Risk Assessment WG and Control Systems Security WG assisted the DOE in development of the Interagency Security Plan. The ES is now embarked on providing individual assistance to the DOE in the drafting of the long term National Infrastructure Protection Plan. The Physical Security of Unstaffed Facilities group is nearing completion of a SG for substations.</p> <p>Risk Assessment WG Control Systems Security WG ESISAC SC</p>
H	32. Implement NERC IT standards.	NERC standards related to physical and cyber security should be understood as being included within the body of standards to be made mandatory and enforceable in Recommendation No. 1.	Assess industry compliance with the NERC 1200 Standard and provide education to assist the industry (as it desires) in

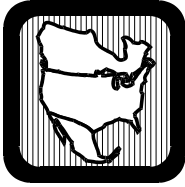
Pr	Recommendation Description	Summary	CIPC Response
		<p>Further:</p> <p>A. NERC should ensure that the industry has implemented its Urgent Action Standard 1200; finalize, implement, and ensure membership compliance with its Reliability Standard 1300 for Cyber Security and take actions to better communicate and enforce these standards.</p> <p>B. CAs and RCs should implement existing and emerging NERC standards, develop and implement best practices and policies for IT and security management, and authenticate and authorize controls that address EMS automation system ownership and boundaries.</p> <p>These actions should include, but not necessarily be limited to:</p> <ol style="list-style-type: none"> 1. The provision of policy, process, and implementation guidance to CAs and RCs; and 2. The establishment of mechanisms for compliance, audit, and enforcement. This may include recommendations, guidance, or agreements between NERC, CAs and RCs that cover self-certification, self-assessment, and/or third-party audit. 3. Work with federal, state, and provincial/territorial jurisdictional departments and agencies to regularly update private and public sector standards, policies, and other guidance. <p>CAs and RCs should develop and implement best practices and policies for IT and security management drawing from existing NERC and government authorities' best practices. These should include, but not necessarily be limited to:</p> <ol style="list-style-type: none"> 1. Policies requiring that automation system products be delivered and installed with unnecessary services deactivated in order to 	<p>increasing their level of compliance. The 1200 Standard initial compliance (reported as of February 2004) was reviewed (not on an entity basis) to determine gaps with respect to specific parts of the standard. The Cyber Members on CIPC and the Outreach WG will recommend the content of a program for the ES.</p> <p>Standards & Guidelines WG Outreach WG</p> <p>Support development of the replacement 1300 Standard.</p> <p>CIPC</p>

Pr	Recommendation Description	Summary	CIPC Response
		<p>improve “out-of-the-box security.”</p> <ol style="list-style-type: none"> 2. The creation of centralized system administration authority within each CA and RC to manage access and permissions for automation access (including vendor management, backdoors, links to other automation systems, and administrative connections). 3. Authenticate and authorize controls that address EMS automation system ownership and boundaries, and ensure access is granted only to users who have corresponding job responsibilities. 	
L	33. Develop and deploy IT management procedures.	CAs' and RCs' IT and EMS support personnel should develop procedures for the development, testing, configuration, and implementation of technology related to EMS automation systems and also define and communicate information security and performance requirements to vendors on a continuing basis. Vendors should ensure that system upgrades, service packs, and bug fixes are made available to grid operators in a timely manner.	The IT expertise on CIPC will assist the Operating Cmte groups as requested, with focus on cyber security matters. The 1200 Standard and SGs apply.
M	*34. Develop corporate-level IT security governance and strategies.	CAs and RCs and other grid-related organizations should have a planned and documented security strategy, governance model, and architecture for EMS automation systems.	CIPC is primarily concerned with the IT systems that are involved in control and monitoring of electric systems and their components. Control Systems Security WG comments on the DOE document “21 Steps to Improve Cyber Security of SCADA Networks” were approved by CIPC at the 09 June 2004 meeting; NERC will forward comments to DOE. A Security Guideline is being prepared to address the 21 Steps that are not covered in the 1200 Standard or SGs. Pursue this recommendation with the compliance and awareness related to the 1200 Standard and

Pr	Recommendation Description	Summary	CIPC Response
			<p>extend to the 1300 Standard.</p> <p>Control Systems Security WG Standards & Guidelines WG Outreach WG</p>
L	35. Implement controls to manage system health, network monitoring, and incident management.	IT and EMS support personnel should implement technical controls to detect, respond to, and recover from system and network problems. Grid operators, dispatchers, and IT and EMS support personnel should be provided the tools and training to ensure that the health of IT systems is monitored and maintained.	<p>Technical support to Operating Cmte groups as requested. Control system intrusion detection (automated and visual by operators).</p> <p>Control Systems Security WG</p>
H	36. Initiate a U.S.-Canada risk management study.	<p>Federal governments should strengthen and expand the scope of the existing risk management initiatives by undertaking a bilateral (Canada-U.S.) study of the vulnerabilities of shared electricity infrastructure and cross border interdependencies.</p> <p>Common threat and vulnerability assessment methodologies should be also developed, based on the work undertaken in the pilot phase of the current joint Canada-U.S. vulnerability assessment initiative, and their use promoted by CAs and RCs.</p> <p>To coincide with these initiatives, the electricity sector, in association with federal governments, should develop policies and best practices for effective risk management and risk mitigation.</p>	<p>Continue to collaborate with governments to develop risk assessment methodologies and solutions applicable to the electricity industry.</p> <p>Consideration being given to establishing a dialog with the ES in US/Canada with ES in Australia, New Zealand, England and a separate dialog with ES in Israel.</p> <p>Risk Assessment WG CIPC EC</p>
L	37. Improve IT forensic and diagnostic capabilities.	CAs and RCs should seek to improve internal forensic and diagnostic capabilities, ensure that IT support personnel who support EMS automation systems are familiar with the systems' design and implementation, and make certain that IT support personnel who support EMS automation systems have are trained in using appropriate tools for diagnostic and forensic analysis and remediation.	<p>Support to Operating Cmte groups. Control system intrusion detection (automated and visual by operators). Consider a workshop topic based upon the documents: "Best Practices for Seizing Electronic Evidence" and "The Silent Witness – Physical Evidence".</p> <p>Outreach WG</p>

Pr	Recommendation Description	Summary	CIPC Response
			Control Systems Security WG
M	38. Assess IT risk and vulnerability at scheduled intervals.	IT and EMS support personnel should perform regular risk and vulnerability assessment activities for automation systems (including EMS applications and underlying operating systems) to identify weaknesses, high-risk areas, and mitigating actions such as improvements in policy, procedure, and technology.	Support to Operating Cmte groups. Enhance existing security guidelines, recommend in 1300 Standard. Standards & Guidelines WG Risk Assessment WG Control Systems Security WG
M	39. Develop capability to detect wireless and remote wireline intrusion and surveillance.	Promote the development of the capability of all CAs and RCs to reasonably detect intrusion and surveillance of wireless and remote wireline access points and transmissions. CAs and RCs should also conduct periodic reviews to ensure that their user base is in compliance with existing wireless and remote wireline access rules and policies.	Control system intrusion detection (automated and visual by operators). Enhance existing Securing Remote Access guideline or develop new guideline. Control Systems Security WG
H	40. Control access to operationally sensitive equipment.	RCs and CAs should implement stringent policies and procedures to control access to sensitive equipment and/or work areas.	Support to Operating Cmte. 1200 and 1300 Standards. Enhance existing guideline and provide education. Develop new SG: Physical Security – Substations. Physical Security of Unstaffed Facilities Task Force. Standards and Guidelines WG Risk Assessment WG
M	41. NERC should provide guidance on employee background checks.	NERC should provide guidance on the implementation of its recommended standards on background checks, and CAs and RCs should review their policies regarding background checks to ensure they are adequate before allowing sub-contractor personnel to access their facilities.	Review and enhance SG: Employment Background Screening. Standards and Guidelines WG Outreach WG
H	42. Confirm NERC ES-ISAC as the central point for sharing security information and analysis.	The NERC ES-ISAC should be confirmed as the central electricity sector point of contact for security incident reporting and analysis. Policies and protocols for cyber and physical incident	Develop ES-ISAC governance structure and recommend enhanced ESISAC capability. ESISAC SC

Pr	Recommendation Description	Summary	CIPC Response
		reporting should be further developed including a mechanism for monitoring compliance. There also should be uniform standards for the reporting and sharing of physical and cyber security incident information across both the private and public sectors.	Indications, Analysis, Warnings WG Outreach WG
L	43. Establish clear authority for physical and cyber security.	Corporations establish clear authority and ownership for physical and cyber security.	Increase awareness at senior management levels. Redo the Business Cases for Action to emphasize Corporate obligations. Outreach WG
M	44. Develop procedures to prevent or mitigate inappropriate disclosure of information.	The private and public sectors should jointly develop and implement security procedures and awareness training in order to mitigate or prevent disclosure of information by the practices of open source collection, elicitation, or surveillance.	Develop broad consensus on sensitive information sharing with government. Utilize the Protecting Critical Infrastructure Information (PCII) and other protective mechanisms and offer suggestions for improvement. Work with the other Standing Committees to assure uniform approach. Review Security Guideline: Protecting Sensitive Data. A NERC response to the existing PCII rules was submitted to DHS by 20 May 2004. Standards and Guidelines WG



North American Electric Reliability Council

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

NERC CONTROL SYSTEMS SECURITY WORKING GROUP RISK ASSESSMENT WORKING GROUP CRITICAL ASSET DEFINITION

The two working groups met during August 2004 and recommend the following for discussion at the EEI Security Committee and NERC Critical Infrastructure Protection Committee at their September 2004 meetings.

The following definition of the term “Critical Asset” for use in NERC Critical Infrastructure Protection (CIP) work is recommended to the CIP Committee (CIPC). If approved by the CIPC, the definition will be made consistent in all existing and proposed Security Guidelines and will be recommended for use by the Cyber Security Standard – 1300 Drafting Team.

“Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.”

Critical Assets

This term is used in the Cyber Security Standard – 1200, the proposed Cyber Security Standard –1300, and several Security Guidelines. A uniform definition is necessary. The term is currently defined in the Security Guidelines for the Electricity Sector Overview:

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

Discussion:

1. The definition of Electricity Sector (ES) critical assets applies to specifically designated facilities within classes such as substations, switching stations, generating stations (exclusive of nuclear), control centers.
2. The definition applies to specifically designated elements within facilities.
3. The definition applies to physical and cyber security.
4. The actual identification of critical assets is the purview and responsibility of the asset owners.

5. Methodologies, appropriate to the various entity types and characteristics, to assist in critical asset identification should be assembled.
6. An ES asset can be identified critical due to bulk electric system reliability requirements. Tools such as the EPRI Transmission Reliability Evaluation of Large-Scale Systems (TRELSS) and the I2R Technologies Electric System Vulnerability Assessment Tool may be useful.
7. An ES asset can be identified critical due to load served. This determination may require collaboration with federal, provincial, state, and local governments.
8. A common definition should be applied to all NERC Security Standards and Security Guidelines. Each specific standard and guideline may further clarify the definition with quantifiers. Ultimately the asset owners must define the appropriate numerics for their own systems because conditions vary greatly.

Security Guidelines for the Electricity Sector: Physical Security — Substations

DRAFT

NERC	Guideline
Guideline Title: Physical Security — Substations	Version: 0.6
Revision Date: August 19, 2004	Effective Date:

Purpose:

Each entity should implement physical security measures at their substations to safeguard personnel and prevent unauthorized access to critical assets, control systems, equipment, and information that may be resident in the substation. Each entity should implement substation security solutions in a way that is consistent with the criticality of the substation and sufficient to provide appropriate situational awareness of activity at these substations so that the entity can initiate an appropriate and timely response.

The NERC document “An Approach to Action for the Electricity Sector” version 1.0 dated June 2001, lists the following as examples of critical infrastructure assets that, if disrupted or threatened, would adversely impact regional, national, or the North American electrical grid reliability:

- important regional transmission hubs,
- interregional tie lines,
- substations that feed interregional ties,
- interregional communications facilities, and
- security [control] centers.

While some of the above facilities are attended around-the-clock to support operations, most are normally unattended. Unattended critical facilities such as substations require appropriate levels of physical security. Many of the security solutions that are readily applicable to attended facilities cannot be readily applied at the unattended substation.

Applicability:

This guideline applies to electric substations. While many substations contain critical assets, some substations are more critical than others to the support of the electricity infrastructure and the overall operation of the power system.

Each entity, using a risk assessment methodology, should define and identify those substations, whether attended or not, it believes to be critical, keeping in mind that the ability to mitigate the loss of a substation through redundancies or operations may make that facility less critical than others.

Security Guidelines for the Electricity Sector: Physical Security — Substations

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

Guideline Statement:

This guideline recommends that “most effective practices” be applied at an appropriate level for electric substations consistent with the level of criticality of the substation as determined by the asset owner. This guideline should be used in conjunction with the Physical Security Guideline and the Vulnerability and Risk Assessment Guideline as well as any other guidelines that apply, which assists entities in identifying critical facilities.

Background:

Attended facilities like control centers, communication facilities, and corporate offices, present a different physical security challenge because they tend to be more complex, centralized, and have multiple physical perimeters. While the more centralized nature of attended facilities allows more economy of scale, this advantage is balanced against the risks associated with common points of failure and cascade effects associated with a single event. Attended facilities also tend to house a great deal more critical cyber assets than the unattended facility. NERC cyber security standards specifically addresses many of the physical security needs of attended facilities in the following sections:

- Physical Security Perimeter[s]
- Physical Access Controls
- Personnel
- Monitoring Physical Access
- Systems Management
- Physical Incident Response Actions

In addition, critical attended facilities typically require many more support assets such as UPS, chilled water, redundant external power supply, environmental controls, and communication infrastructure that the typical unattended facility would not require. Since these support assets are fundamental to the reliable operation of the critical facility, they are themselves critical assets and require appropriate physical protection.

Unattended facilities like substations are common elements in the electric industry. Substations contain many of the fundamental critical assets necessary for the transmission and distribution of electric power to customers. Transformers, breakers, busses, switches, capacitor banks, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Intelligent Electronic Devices (IEDs), and communication systems can reside within the confines of the substation. The compromise of any one of these elements can impact the integrity of the electric grid, depending on the amount and type of load being served by this substation at the time of the incident.

Security Guidelines for the Electricity Sector: Physical Security — Substations

While the substation is in many ways the “neuron” of the electrical network allowing effective monitoring and control of electric energy in that particular area of the network, they are attended for very short periods of time. Unlike control centers and most power plants that are staffed around the clock, there is typically no staffing, limited or no roving security patrols, and roofed structures are typically designed to protect electronic equipment and switch gear. Typically, substations outnumber power plants 30:1 and can be located in a downtown setting or in the most remote of rural areas. While most critical substations will logically be located in or near major load centers, interregional ties located in remote substations may be just as critical for interconnection purposes.

Substations are located in urban, suburban, rural, and industrial/commercial sites and the effectiveness of security methods differs greatly from site to site. Because of the diversity in substation size, location, and criticality, each substation should be assessed and classified. In general, more rigorous security measures should be applied to the more critical substations. While all substations are a critical element in the transmission and distribution of electric energy, not all substations are equally critical to North American electric grid reliability.

This guideline is intended to provide suggestions when considering the physical security at substations with a focus on practical methods using existing technology and proven processes. All of the security methods discussed here can be applied to existing substations.

Definitions:

Entity — The facility or asset owner, operator, etc.

Critical Asset — Those facilities, systems, and equipment which, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

Intruder — Any unauthorized individual or any individual performing unauthorized activity within the substation.

Physical Security Perimeter — A type of gate, door, wall, or fence system that is intended to restrict and control the physical access or egress of personnel.

Security Assets — Fences, gates, alarm systems, guards, and other security elements that can individually or as a system be applied to critical electrical assets to maintain reliability or reduce risk.

Substation Secure Area — The area contained within the first or outer substation physical security perimeter.

Security Guidelines for the Electricity Sector: Physical Security — Substations

Guideline Detail:

Physical security typically comprises five distinct elements, or systems:

- Delay/Deterrence
- Detection
- Assessment
- Communication
- Response

Together, these elements provide a consistent “systems approach” to protecting critical assets. While the application of these five elements will differ between substations, they all apply to some degree.

Each entity should prioritize its substations and associated assets. This prioritization should consider risks based on factors such as prior history of incidents, threat warnings from law enforcement agencies, loss of load consequences, response time, recovery time, and overall operating requirements. Each entity also should consider an inspection and assessment program to review existing security systems at substations and to make recommendations for appropriate changes. (See guideline for conducting vulnerability assessments.)

General Guidelines:

The details included below can generally be implemented with currently available technology. Many of these solutions are also discussed in the Physical Security Guideline:

1. fencing and gates to restrict access to the facility for both safety and security purposes;
2. limiting access to authorized persons through measures such as unique keying systems, “smart locks,” access card systems, or the use of security personnel;
3. access control measures to identify and process all personnel, visitors, vendors, and contractors, (i.e., photo ids, visitors passes, contractor ids) to be displayed while in the substation;
4. alarm systems to monitor entry into substation grounds;
5. perimeter alarm systems to monitor forced intrusion into and surveillance of the substation;
6. alarms, CCTV, and other security systems reporting to an attended central security station that can then be evaluated and entity personnel or law enforcement authorities dispatched to investigate a potential problem;
7. guards (special events or targeted substations);
8. vehicle barriers;
9. adequate lighting;
10. signage;
11. a comprehensive security awareness program.

Security Guidelines for the Electricity Sector: Physical Security — Substations

Physical security systems should be augmented in accordance with the “Threat Alert System and Physical Response Guidelines for the Electricity Sector” based on changes in threat levels, scenarios, and categories. In designing a physical security system, the objective of the intruder should be considered. The four major objectives in describing an intruder’s behavior are:

- Damaging, operating, or tampering with substation equipment and controls,
- Stealing or damaging substation equipment, materials, or information,
- Posing a threat to the safety of entity personnel or customers,
- Creating adverse publicity.

Specific Guidelines:

1. Each entity should have a role-based substation security policy and procedures in place to manage and control access into and out of the substation. These policies should clearly state what practices are prohibited, which ones are allowed, and what is expected of all personnel with access to the substation. The substation security policies should clearly define roles, responsibilities, and procedures for access and should be part of an overall critical infrastructure protection policy.
2. The physical security perimeters at each substation should be clearly identified. All physical access points through each perimeter should be identified and documented. Most substations typically have at least two physical security perimeters such as the fence and the control house building. All access points through the substation fences and substation control houses should be identified.
3. Physical access controls should be implemented at each identified perimeter access point. Where appropriate, all access into and out of the substation should be recorded and maintained for a period of time consistent with NERC standards. At minimum, these records should indicate the name of person(s) entering the substation, their business purpose, their entity affiliation, time in, and time out.
4. Where appropriate, access into and out of the substation should be monitored with authorization procedures. Substation access may be authorized by the system or security operator if not performed by electronic means such as a card reader where authorization is predetermined. Even if card readers are in place, it is recommended that personnel entering the substation contact the system or security operator so that the station can be tagged as “attended” in the event of an incident.
5. Records that identify all entity, contractor, vendor and service personnel that have unescorted access privileges to substations should be identified and documented. While most entity personnel will have unescorted access to all substations, contractors and vendors should only have unescorted access to substations they have contractual business in.
6. Where appropriate, all contractors and vendors with substation access privileges should be required to pass a background screening before being issued an entity-provided contractor ID badge. Only those contractors with entity-issued ID badges should be granted unescorted substation access. Even in these circumstances, an entity employee

Security Guidelines for the Electricity Sector: Physical Security — Substations

with unescorted access to the substation should confirm and monitor the contractor's activity while in the substation appropriately.

7. A substation incident response program should be established that at a minimum would provide a rapid assessment of events in the substation in order to differentiate normal electromechanical failures from malicious acts. If malicious activity is evident, the priority should be to notify law enforcement and return the substation to normal functionality while preserving forensic evidence where possible.
8. Entities should avoid dual use of critical substation grounds for non-critical functions where possible. That is, eliminate or restrict the use of the substation secure area for non-critical activities such as equipment storage, non-critical asset storage, contractor staging, and personal vehicle parking. If dual use is unavoidable, the entity should consider the establishment of another physical security perimeter that excludes the non-critical activities from the substation secure area, or the entire area should conform to this security guideline.

Security Asset Matrix Example:

As stated earlier, each entity should perform a risk assessment on all substations and prioritize each substation based on their own criteria for threat, vulnerability, and consequences. The security asset matrix example below is intended to illustrate how various substation security solutions might be applied. Because this security asset matrix example is intended to be an illustration only, three categories of substations are used for simplicity. In fact, most entities may find additional categories and security assets more useful. For the purposes of this security asset matrix example, Category 1 is a most critical substation, Category 2 is a moderately critical substation, and Category 3 is a least critical substation.

Security Asset Matrix:

Security Assets	Category		
	1	2	3
Card Key	▲		
Special Locks	▲	▲	▲
Security Guard (roving)	▲		
Fence	▲	▲	▲
CCTV	▲		
Door & Gate Open (SCADA)	▲	▲	
Alarm System	▲		
Motion Detectors	▲	▲	

While the security asset matrix example above appears static, the specific security solutions applied to each category of substation should be adjusted as needed to respond to relevant specific threat information.

Security Guidelines for the Electricity Sector: Physical Security — Substations

Substation Security Assets:

Card Keys — A means of electronic access where the access rights of the cardholder are predefined in a computer database. Access rights may differ from one physical perimeter to another.

Special Locks — These may include locks with non-reproducible keys, magnetic locks that must be opened remotely, and possibly some sort of interlock system that restricts access through one perimeter while another is open.

Security Guard (roving) — Either staff or contract security personnel may randomly patrol multiple facilities. This asset is typically used for special events, periods of high threat levels, areas experiencing high intrusion levels, or substations that serve as a staging area for construction.

Fence — This is the minimal security asset and usually defines the first physical security perimeter encountered at the substation. There are several levels of fencing ranging from solid material, to standard chain link fencing (most common), to cable reinforced chain link fence.

CCTV — CCTV can be very effective in substation settings. Examples of pre-processed video surveillance that “cans” or captures images of activity in the substation preceding a substation security alarm can provide the system operator or security operator a “quick review” of the substation without requiring an operator to monitor traditional CCTV screens in real time.

Door & Gate Open (SCADA) — These alarms are typically based on some sort of “contact status” that indicates a door or gate has been opened. These alarms are particularly useful when used in conjunction with some sort of “attended station” status. Note: While these alarms, if received via SCADA, at most will represent only a handful of additional status points for the most critical substation, appropriate attention to RTU scan loading should be considered.

Alarm System — These systems typically incorporate several security solutions into a surveillance and alarming package. These package solutions are usually specific to a high-risk substation, do not interface with any other system, and are set up to provide enhanced forensic evidence at that site.

Motion Detectors — These devices use various means to detect motion in a specific area. While the IEEE’s Standard 1402–2000 lists motion detectors as very effective in almost all sites, these systems can generate false alerts due to the open substation environment.

Exceptions:

None

Security Guidelines for the Electricity Sector: Physical Security — Substations

Certified Products/Tools:

None

Related Documents:

Security Guidelines for the Electricity Sector: Guideline Overview

- Physical Security
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Continuity of Business Processes
- Communications
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

IEEE Guide for Electric Power Substation Physical and Electronic Security, IEEE STD 1402-2000, January 2000.

Threat Alert System and Physical Response Guidelines for the Electricity Sector: Definitions of Physical Threat Alert Levels; A Model for Developing Organization Specific Physical Threat Alert Level Response Plans, Version 2.0, October 8, 2002.

Internet links:

- *Security Guidelines for the Electric Sector* <http://www.esisac.com/library-guidelines.htm>
- *Urgent Action Cyber Security Standard*, NERC, August 13, 2003, <http://www.esisac.com/library-guidelines.htm>
- *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, <http://www.esisac.com/library-other.htm>
- *Threat Alert Levels and Physical Response Guidelines*, NERC, October 2002, <http://www.esisac.com/library-guidelines.htm>

Security Guidelines for the Electricity Sector: Physical Security — Substations

Revision History:

Date	Version Number	Reason/Comments
5/17/2004	0.01	Split out this draft into a separate guideline from the Physical Security Guideline and made several grammatical and content changes.
6/7/2004	0.02	Various wording changes. Added page numbers, alarm system description, and removed several Internet links.
7/1/2004	0.03	Minor wording changes. Omission of “projectile barriers” from page 5. Swap categories 1 & 3 on page 7. Change “CCTV” description on page 7.
7/20/2004	0.04	Various grammatical changes. Replace “must” with “should” where appropriate. Separated matrix example better. Introduced reference to Threat Alert System and Physical Response Guidelines for the Electricity Sector. Defined Intruder. Eliminated surveillance in Item 5 Under General Guidelines. Replaced “three years” with “consistent with NERC Standards”.
8/16/2004	0.05	Various wording and grammatical changes. Altered definitions of critical facility and critical asset to more closely match the definition in the NERC Overview Guideline. Changed all references to company to entity. Returned security elements to original order. Added “Where appropriate” to specific guidelines.
8/19/2004	0.06	Removed “bulk” from applicability. Removed construction from Specific Guideline 8.

Security Guidelines for the Electricity Sector: Cyber — Patch Management

NERC	Guideline
Guideline Title: Cyber — Patch Management	Version: 0.2
Revision Date: April 26, 2004	Effective Date: April 26, 2004

Purpose:

The purpose of this guideline is to provide recommendations for an effective patch management strategy. Patch management is a set of processes used to help alleviate many of the challenges involved with securing computing systems from attack and maintaining availability.

Patch management tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required.

This document provides guidance in the subject area, underscores the importance, and identifies resources in this area.

Applicability:

This guideline is applicable to anyone who owns and/or manages information systems 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.

While everything in this guideline is voluntary, some of the recommendations are more important than others. For this reason, the terms “shall” and “should” are used throughout this document. The term “shall” is used in the more important aspects of this guideline to stress their importance to the overall process. The term “should” is used to indicate the less important aspects of this guideline.

Background:

Regulatory pressure has now made patch management on critical systems a requirement. Consequently, NERC’s Urgent Action Cyber Standard, in Section 1212 — System Management, requires policies and procedures to address Security Patch Management.

Having a patch management strategy does not guarantee a fool-proof environment. Any of the following factors can invalidate the process:

Security Guidelines for the Electricity Sector: Cyber — Patch Management

- Patches that are not identified and installed in time to prevent damage
- Vulnerable systems that were not patched when the patch was deployed
- Defective patches that do not properly close the vulnerability
- Defective patches that create new vulnerabilities, or cause loss of services

However, one area that patch management does address is to demonstrate an entity's commitment to maintaining a secure environment. It assures regulators and key stakeholders the entity is taking reasonable and prudent action in preventing an attack and maintaining reliable service.

Guideline Statement:

The process of patch management includes four areas for implementation. They are asset inventory, vulnerability notification, vulnerability risk assessment, and mitigation strategies. All critical computer systems that could potentially affect the reliability of the grid shall have a formal patch management process.

Guideline Detail:

Asset Inventory:

A successful patch management program includes a comprehensive and centralized asset inventory system. Said system further includes detailed classifications of the entity's asset pool, by order of criticality (prioritization) throughout the infrastructure. At a minimum, all critical cyber assets identified in Section 1202 of the NERC Urgent Action Cyber Security Standard shall be included in the asset inventory system, with the appropriate classification prioritization category.

A significant challenge in accomplishing any successful patch management cycle is the order in which each asset (or group of assets) is addressed. Consequently, when considering the classification of IT assets, in the context of a patch release process, one must also consider communications with, and approvals from the asset's owner. A well-defined classification scheme should reduce the approval time required to deploy security patches to broad groups within an entity's IT infrastructure. Examples of asset classification priority categories might include:

- Early Adopters
- Business Functional
- Business Critical
- Internet/DMZ
- "At Will"
- "Coordinate Schedule"
- "No Touch"

Security Guidelines for the Electricity Sector: Cyber — Patch Management

Vulnerability Notification:

There are many resources available for patch notification used by electric utilities to obtain information for vulnerabilities and the availability of patches to remediate those vulnerabilities.

It is important that each organization considers their unique requirements and builds a comprehensive plan. Critical to the success of patch management is notification and coordination of information. Multiple sources of patch information will exist within an organization. The security group will get vulnerability alerts and notifications on security patches. However, the information technology organizations responsible for the infrastructure, database, and applications should also get this same information.

A focal point for vulnerability alert and patch management coordination should exist. Centralized problem/change management organizations have been utilized in some utilities to provide this coordination point. Problem Management should be a 24-hour/7 day a week operation so vulnerability alerts can be triaged and the appropriate personnel notified to complete an assessment of the vulnerability.

Subscription services are available from the hardware and software vendors as well as third parties. Each utility will need to decide which notification procedures are appropriate for their particular organization. Considerations that will govern the selection of notification procedures are:

- Diversity of hardware and software deployed
- Organizational model for IT (Centralized or distributed)
- Funding available for notification services
- Asset inventory (hardware and software)

Vulnerability Risk Assessment:

Assessing vulnerability risk is typically assigned to a team consisting of technical staff across various platforms and applications. Members may include information security, network administrators, Intel server administrators, UNIX server administrators, workstation support, database support, and applications support. The process shall include steps to identify the risk, assess the risk, and assign responsibility for the appropriate resolution. Examples of risk assessment categories include: Critical, High, Moderate, and Low.

The patching policy should address the acceptable time frame for a patch to be deployed based on the asset classification prioritization category and the risk assessment.

Although a team is formed to assess vulnerabilities, an organization shall establish a person with overall accountability. The title of this person varies across the information

Security Guidelines for the Electricity Sector: Cyber — Patch Management

security industry (e.g., CIO, CSO, CISO, Information Security Manager, etc.) but the main concept is to assign accountability to someone closely associated with information security.

Mitigation Strategies:

Some process control systems are proprietary, and modifications, including patch updates, must be made by the application vendor. Other applications are maintained by the organization, but modifications can only be safely made after the vendor has evaluated and tested the code. This environment presents challenges when “security” patches must be applied. Some mitigation strategies that should be utilized when the application or underlying infrastructure cannot be patched in a timely manner are:

Isolation (Perimeter within Perimeter) — Process control systems should be protected behind a secondary firewall within the utility’s wide area network (WAN). This is in addition to the firewall that separates the WAN from the Internet. In essence, the process control system is protected in a perimeter within a perimeter. The secondary firewall can limit network traffic in a more granular fashion than the Internet firewall. Intrusion detection devices can be used to monitor the process control perimeter. Intrusion Detection Systems (IDS) designed for industrial control networks are becoming more readily available and feasible across the industry.

Hardening — Only those “services” of the Operating System (O/S) required by the process control application should be enabled on its servers. Unused protocols and services should be disabled and noted. Periodic review of said changes should be conducted to ensure that the services are not inadvertently re-enabled.

Adopting minimum baseline standards ensure that you are not needlessly patching. This means turning off all extraneous services. Thus, review how the device will be utilized and turn off all services that do not support a specific business need. The operating system vendors such as Microsoft or network routing equipment vendors such as Cisco should provide technical support and guidance.

Independent third parties such as the Sans Institute (www.sans.org) can provide valuable guidance. Another source is the National Security Agency (NSA) website (www.nsa.gov). The NSA currently offers secured configuration recommendation guidelines for the following products: Windows XP, Windows Server 2000 and 2003, Windows NT, guides for Cisco routers, e-mail and executables, Microsoft Internet Information Services 5.0, & Solaris.

Assets configured to the appropriate baseline level should be scrutinized in a separate testing environment for appropriate functionality before being deployed into production.

Security Guidelines for the Electricity Sector: Cyber — Patch Management

Temporary Isolation (based on CIPC or entity determined threat level) — Traditionally, many utility process control systems were “air-gapped”. They were islands unto themselves, not connected to the entity Wide Area Network, to the Internet, or to any other of the organization’s network. This has changed recently and connectivity, although tightly controlled through firewalls and the use of encryption (VPN tunnels), occurs frequently.

In certain situations, the process control system should be temporarily disconnected from any other networks. This is the appropriate strategy in a “Day 0” scenario. (Day 0 refers to a virus or worm that is newly discovered in the wild and for which virus protection signatures and patches are not yet available.)

Access Control — Access Control was not rigorously enforced in the traditional “air-gapped” systems. In today’s interconnected environment, it is very important that each process control system user be uniquely authenticated before access is granted. Connectivity to external organizations is another example of access control. These connections should each be separately evaluated by the information technology security group. Specific language, including, but not limited to, non-disclosure agreements, must be included in the contract that governs the relationship(s) requiring such connectivity.

Exceptions:

None, unless a waiver is approved by the information security manager.

Certified Products/Tools:

Numerous

Glossary:

SCADA: Supervisory Control and Data Acquisition — Systems are used in industry to monitor and control plant status and provide logging facilities. SCADA systems are highly configurable, and usually interface to the plant via PCLs.

CERT: Established in 1988, the CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Process Control Systems: (NOTE: Need a good standardized NERC definition here)

Security Guidelines for the Electricity Sector: Cyber — Patch Management

Related Documents:

- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
 - Vulnerability and Threat Assessment
 - Threat Response
 - Emergency Plans
 - Continuity of Business Processes
 - Communications
 - Physical Security
 - Cyber Security
 - Employment Background Screening
 - Protecting Potentially Sensitive Information
- Urgent Action Standard 1200 Cyber Security, NERC, August 13, 2003, <http://www.nerc.com/cip.html>
- NIST Special Publications, NIST documents of general interest to the computer security community, <http://csrc.nist.gov/publications/nistpubs/index.html>
- Vulnerabilities, Incidents, and Fixes, CERT, http://www.cert.org/nav/index_red.html
- United States-Computer Emergency Readiness Team (US-CERT), <http://www.us-cert.gov>
- Computer Incident Advisory Capability, U.S. Department of Energy, <http://www.ciac.org/ciac/index.html>
- The SANS Institute, <http://www.sans.org>
- Bugtraq Archive, SecurityFocus, <http://www.securityfocus.com/archive/1>
- Patch Management Strategies for the Electric Sector, Edison Electric Institute, March 2004, <http://www.eei.org>

Revision History:

Date	Version Number	Reason/Comments
4-26-2004	Version 0.1	<i>Draft 1 developed from original EEI White Paper for Patch Management Strategies</i>



NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

August 26, 2004

Department of Energy

Dear

Comments and Suggestions for Consideration by the Department of Energy on the Second Release of the “21 Steps to Improve Cyber Security of SCADA Networks”

The Control Systems Security Working Group, a subgroup of the North American Electric Reliability Council’s Critical Infrastructure Protection Committee (CIPC), has solicited comments and suggestions on your second release of the “21 Steps to Improve Cyber Security of SCADA Networks” for your consideration. Although the currently published version of this document is informative and helpful, the group believes that some revisions could enhance it, thereby making it more useful to a greater population. The following comments and suggestions are offered for your consideration together with our recommendation that the Department of Energy should revise and release a new version of this document every two years. The CIPC is also drafting a “Security Guideline for the Electricity Sector: Secure Connectivity of Control Systems” that will be published on the NERC website to supplement the DOE document.

1. Change all references from SCADA networks to Control Systems. This will broaden the scope of the suggestions to encompass more of the critical cyber assets and the suggestions apply to more than just the SCADA networks.
2. Make reference to the NERC standards, guidelines, and white papers.
3. Recognize that legacy control systems may not be compatible with some of these recommendations and indicate that those systems should comply to as great a degree as possible, or suggest other additional mitigating processes.
4. In step one, include some additional types of connections: RTUs, IEDs, PLCs, station computers, relays, microwave and/or base radio, and plant control systems. Consider a simple, unambiguous architecture to govern all connectivity.
5. In step two, add “apply security recommendations made by appropriate professional and standards organizations.”
6. In step three, highlight the importance of protecting all of the communication and equipment at remote facilities. Also suggest removing the suggestion to perform penetration testing. Non-invasive testing approaches need to be followed.

Mr.
August 26, 2004
Page Two

7. In step four, review your examples of services that should be disabled. Some services that are needed for remote maintenance and administration are necessary for field resident equipment and may need other hardening techniques such as using a Virtual Private Network.
8. In step five, more emphasis needs to be placed on the vendor's disclosure responsibilities.
9. In step six, suggest contractual arrangements with vendors to encourage them to redesign their systems not to rely on default, insecure computer settings. Asset owners should include security specifications in negotiated arrangements.
10. In step seven, suggest that asset owners need to confirm whether or not back doors exist (see step one identify all connections) and consider means for managing access through those back doors and institute a process for enabling access only when needed.
11. In step eight, add a clarification that Intrusion Detection should be implemented "where applicable;" highlight that Intrusion Detection may create unacceptable overheads and suggest network layers of security architecture may be necessary instead.
12. In step nine, recognize that many commercial IT system tools and policies may not be appropriate for control systems.
13. In step ten, add wording to address unescorted access in protected areas and establishing policies to prohibit the use of recording equipment (e.g, camera phones and PDA devices, etc.) unless previously approved by management.
14. In Step eleven, "Red Teams" may not be the appropriate solution.
15. In Step twelve, also define the communication flow within the organization as part of the roles and responsibilities during and after an incident.
16. The documentation suggested in step 13 should include whether or not the device is providing a critical function; documentation should be prepared at the appropriate level of detail for the intended audience.
17. Step fourteen should mention that change management should be part of the risk assessment task.
18. Step eighteen should suggest that organizations conduct routine assessments, rather than self-assessments. (Some organization may choose to use outside resources to conduct those assessments.) Organizations should consider establishing a Threat Response Plan that unambiguously states the security processes that should be in place at each threat level.

Thank you for considering our suggestions. Please advise if we can provide additional clarification and assistance. Our point of contact is: Linda Nappier, AMERN (314-554-3595)

Sincerely,

Top 10 Vulnerabilities of Control Systems
19-Aug-2004 version

Categories: boundary security, access administration, design considerations.

List of vulnerabilities. Reviewed periodically. Utilized by asset owners in their risk management process. ...

1. Lack of sufficient defense in depth and communication compartmentalization with the “entity” network. Poorly designed control networks (i.e. recognizing the specific criticality of controls). Unprotected communications. Excessive dependence on “security by obscurity”. Remote trusted access.
2. Lack of understanding of system configurations, including embedded system devices. Misconfiguration of operating parameters. Patches not current. Concern for testing patches before inserting.
3. Protocols are not authenticated between terminals.
4. Use of inappropriate wireless communication. Lack of two way authentication in 802.11 wireless communications and management.
5. Internet based SCADA. Use of non-deterministic communications for command and control.
6. Remote administrative/maintenance access. / Out of band (i.e. modems) access. Remote access password control: some cannot be changed; some are just not changed; some the owner may not even be aware of. Limited use of VPN in control systems due to maintenance issues. Key management.
7. Lack of methods to analyze intrusions; to know the difference between a legitimate vs. unauthorized command (or data).
8. Bandwidth over-usage (e.g. via worm, non-prioritized download), may lead to loss of control. Lack of control may be as bad as compromised control.
9. A significant vulnerability might be lack of boundary checks in control systems (i.e.: control signal or data input is outside reasonable numerical bounds).
10. Implementation of unauthorized software.