Rev. 4.0; 2/25/02

NIPC-EP/ISAC

INDICATIONS, ANALYSIS & WARNING PROGRAM

STANDARD OPERATING PROCEDURE (SOP)

NIPC-EP/ISAC
INDICATIONS, ANALYSIS & WARNING PROGRAM
STANDARD OPERATING PROCEDURE (SOP)

1. PURPOSE:

This SOP establishes voluntary procedures for implementing the information reporting, analysis and warning provisions of the National Infrastructure Protection Center's (NIPC) national-level Indications, Analysis & Warning (IAW) program for electric power. This program has been established to enable the NIPC to provide timely, accurate, and actionable warning for both operational and cyber threats or attacks on the national electric power infrastructure. No procedure established by this Standard supercedes existing mechanisms and channels for reporting company incident data to the FBI, RCMP or other law enforcement agencies.

2. BACKGROUND and OVERVIEW:

Presidential Decision Directive (PDD)-63, signed on May 22, 1998, authorized the creation of a full scale National Infrastructure Protection Center (NIPC). The PDD tasked the NIPC to serve as the national critical infrastructure assessment, warning, vulnerability, and law enforcement entity. Further, it directed all executive departments to share information with the NIPC about threats, warnings and actual attacks on critical government and private sector infrastructures to the extent permitted by law. In addition, it authorized the NIPC to establish its own relations directly with others in the private sector and with any information and analysis entity that the private sector may create.

To fulfill one portion of its assessment and warning mission as assigned by the PDD and with the assistance of government officials and industry representatives from the electric power sector, the NIPC has developed general guidelines for reporting voluntarily any operational and cyber incidents adversely affecting the nation's electric power infrastructure. Reporting entities are expected on a voluntary basis to provide the NIPC with information on unscheduled service outages, degraded operations and serious threats to facilities, activities and information systems, provided they meet established reporting criteria and thresholds as defined in *Indications, Analysis & Warning [IAW] Criteria and Thresholds for Reporting Incidents Affecting Electric Power* (see Attachment A).

Following receipt of standardized incident reports from the electric power and other infrastructures, the NIPC will process and evaluate the information and will disseminate

timely and actionable assessments, advisories and alerts[1] to appropriate government and private sector entities when such incidents are deemed to have possible serious national security, economic or social consequences.

Comments on this SOP should be addressed to the NIPC Watch & Warning Unit (ATTN: IDSU Unit Chief) by telephone (202-323-3204, -3205, -3206), FAX (202-323-2079, -2082), or email (nipc.watch@fbi.gov).

3. APPLICABILITY:

This SOP is intended to apply to all entities engaged in the provision of bulk or retail electric power services (i.e., generation, transmission, control, power marketers, and distribution for specific locations associated with national security or emergency preparedness –NS/EP—customers).

This SOP is not entered into as a legally binding agreement, nor is it a formal expression of a legally binding agreement, but it is an expression of purpose and intent of the parties concerned. Similarly, this SOP does not confer, grant or authorize any rights, privileges, or obligations. This SOP is not an obligation or commitment of funds nor a basis for a transfer of funds.

4. RESPONSIBILITIES:

A. The NIPC ISAC[2] Development & Support Unit (IDSU) is responsible for:

1) Proper implementation of and compliance with this SOP within the NIPC.
2) Ensuring that incident reports received by the NIPC pursuant to this SOP are processed in near real-time, and that timely and actionable warning notices are disseminated to appropriate Government and industry IAW participants, with protections applied to the proprietary and/or sensitive nature of such information.
3) Maintenance of this SOP.

B. As the designated ISAC for the electric power industry, the North American Electric Reliability Council (NERC) is responsible for establishing the voluntary basis for:

1) Reporting to the NIPC by individual entities, system operators or security coordinators (as appropriate) incidents from malicious or unknown causes that meet the criteria defined in Attachment A.

---

[1] **Assessment**; broad, general incident or issue awareness information and analysis that is both significant and current but does not necessarily suggest immediate action.
Advisory; significant threat or incident information suggesting a change in readiness posture, protective options and/or response.
Alert; major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

[2] Information Sharing and Analysis Centers, as called for in the PDD, to be established by each critical infrastructure to focus and communicate its security assurance activities.

2) Assistance by cleared NERC staff and other designated industry personnel to work with NIPC to declassify threat and warning messages to permit broader dissemination.
3) Having experts available (e.g., security coordinators) to consult directly with the NIPC on selected incident reports when appropriate for specific assessments.
4) Assuring that an up-to-date version of the SOP is available on the NERC web-site.

C. All industry and government entities participating in the program are expected to report, on a voluntary basis, to the NIPC Watch & Warning Unit information pertinent to incidents or threats affecting the generation, transmission, delivery, control, or distribution of bulk or retail electric power in accordance with the reporting criteria and thresholds established and set forth in Attachment A to this document.

5. INCIDENT REPORTING:

STAGES. Reporting of events meeting the guidelines in Attachment A is strongly encouraged when the cause is **known** or **suspected to be** of malicious origin. Reporting of events where the cause is uncertain or unknown is also strongly encouraged (i.e., still uncertain or unknown beyond the time periods designated by the criteria in Attachment A). Reporting is not necessary if it is considered highly probable that the cause is **NOT** of malicious origin, or until such time that a reportable cause is established.

Reporting is divided into three separate stages in recognition of the need for timely notification to the NIPC, the likely time required for operating personnel to investigate and resolve an incident, and the need to minimize reporting burdens on industry. A standardized format for reporting all three stages of incident data has been developed and is included as Attachment B hereto (NIPC Incident Report-Electric Power); up-to-date copies will be maintained on the secure NERC web-site[3]. At each subsequent stage, as defined below, it is anticipated that personnel submitting incident reports will be able to provide more complete and definitive information until, finally, at Stage 3, the incident will be effectively closed out. At any time, originators may terminate reporting on any incident determined to lack malicious intent by so changing the entry in block #7 (Cause of Outage/ Degraded Operation), Section 1 of the Incident Report Form and sending a revised report to the NIPC.

- Stage 1 Report: The first report is intended to provide notice that an incident meeting one or more of the criteria and thresholds described in Attachment A has occurred. Stage 1 reports are requested immediately following the first 60 minutes after detection of an incident.

[3] Access may be granted by NERC CIP Program Manager; (609) 452-8060.

In some cases, respondents may be unable to determine the exact nature of anomalous events on their systems or whether any of the incident criteria have been met. In these cases, an abbreviated Stage 1 Report can be filed by providing known information in the "Additional Comments" section at the end of the Stage 1 Report. Aside from originator profile information, other Stage 1 entry categories may be left blank.

Unless otherwise indicated in Attachment A, reports should be filed by the entity detecting the incident(s).

- Stage 2 Report: Using the same reporting format, these reports are requested within 4-6 hours after submittal of the initial (Stage 1) report when more complete information is generally available.

- Stage 3 Report: This third and last report will be filed only for malicious events and will represent the final entry for the incident report. It should contain all relevant facts that can be determined within a 60 day period following filing of a Stage 1 report, or on a closeout schedule established by the originator and filed with the NIPC.

REPORTING. To secure the broadest participation in the IAW program, the standard Incident Reporting Format (Attachment B) resides on and can be used to report incidents through the FBI's secure InfraGard web-server. It features a document template and, once filed, will return to the originator a unique identification number for that particular filing.

Additionally, incident reports can be sent by the originator to the NIPC Watch & Warning Unit using the email or FAX addresses shown on the reporting form, or relayed to the NIPC by the ISAC Information System.
.

1. INCIDENT DATA TO BE REPORTED:

An incident report will be submitted, generally by electric power operators or Security Coordinators, for events meeting criteria and satisfying the thresholds shown in Attachment A. Report filings will be submitted in the format established in Attachment B. Filings may be sent either non-secure, to the NIPC.Watch@fbi.gov, or secure, by sending sensitive information to the NIPC via the FBI's secure InfraGard web-server or by encrypted email procedures established by InfraGard.

2. RECEIPT AND PROCESSING BY THE NIPC:

All reports will be received at the NIPC Watch &Warning Unit (7x24), immediately logged, assigned a unique identification number, and acknowledged to the originator. It will then be integrated into an IAW incident database and made available to appropriate

NIPC analyst servers and/or databases observing established protocols to protect sensitive information. Incident Reports designated by their originators as 'Public' are releasable without further restrictions. Those designated as 'Proprietary' or 'Confidential' are releasable either to: 1) other Infragard members who have signed the Secure Access Agreement; or, 2) authorized personnel at NERC, NERC Security Coordinators and NIPC/FBI depending on the selection chosen by the originator. Those designated 'Proprietary' or 'Confidential' will be maintained by the NIPC as exempt from disclosure under the Freedom of Information and Trade Secrets Acts.

A. CONFIRMATION OF RECEIPT OF INFORMATION AND THAT EVENT(S) MEET REPORTING THRESHOLD(S). NIPC Watch Unit personnel will send a reply to the originator assigning a unique identification number and indicating receipt of the report. The NIPC then will examine the incoming data report to verify that the incident being reported does in fact meet one or more of the threshold criteria listed in Attachment A.

B. RESOLVING QUESTIONS ABOUT INCIDENT REPORTS. The NIPC sincerely intends to minimize reporting burdens on operating system personnel who, in addition to the press of actual system operations activities, are likely to have their hands full attempting to restore service and recover from consequences produced by reported incidents. To accomplish this objective and yet render effective and timely assessment, assigned NIPC analysts may contact appropriate Security Coordinators and/or NERC staff to resolve questions concerning any of the associated facts and/or possible relationships to other contemporaneously reported incidents.

C. ANALYSIS OF INFORMATION AND DETERMINATION OF WHETHER TO SEND OUT WARNING NOTIFICATION. The NIPC will evaluate information filed by members of the electric power infrastructure, compare it with similar information submitted by entities from other critical infrastructures and federal/state agencies and attempt to determine whether a coordinated attack is underway against U.S. national interests. The emphasis of this SOP is on tactical analysis and response based on information likely to be available in a timeframe to support a warning function. The purpose of this NIPC tactical analysis and response activity is *to provide 'actionable' warning notification of threats and impending attacks on critical infrastructures to prevent or mitigate consequences*. This information, when it appears to pertain to the commission of a crime, could also be used by FBI field offices to identify, apprehend and prosecute perpetrators. Company assent is required for the field office to open an investigation.

D. ACCESS TO/DISSEMINATION OF INCIDENT REPORTS. Information contained in incident reports may be labeled by their originators in one of the following three categories: 1) Public Information-available for public dissemination without restriction; 2) InfraGard Secure Information/PROPIN- proprietary and available only to members that have signed the InfraGard Secure Access Agreement; 3) NERC-NIPC Security Data/PROPIN-proprietary information available only to the NIPC, NERC and to entities designated by NERC.

3. DISTRIBUTION OF WARNING NOTIFICATION:

Some of the information available to the NIPC may be classified or law enforcement sensitive and, thus, unavailable to many in industry. A select group of NERC officials and other designated industry personnel is being sponsored for clearances by, and at the expense of, the NIPC and will be provided with the means to access classified material. The purpose of this group will be to advise the NIPC on matters of declassifying and sanitizing warning material so that it may be disseminated to all appropriate personnel industry-wide and yet retain actionable content. Once the NIPC has determined that a warning should be issued, all or a sufficient subset of these advisors will be available as needed to assist the NIPC in sanitizing and finalizing warning notices so as to provide non-proprietary, timely and *actionable* information to the maximum extent possible.

The table (below) describes the plan envisioned by this SOP for disseminating warning products.

Class of Information:	Distribution Media:	Recipients:
Classified	-STU-3 -Secure FAX -Secure teletype	Participating industry and government personnel with appropriate clearances and need-to-know for each particular incident.
Limited Distribution • InfraGard "Secure Information" • Other information in accordance with submitter's restrictions	Secure InfraGard web server and email Email or fax via NERC	InfraGard Members with signed Agreement Electric Power entities
Public	NIPC public web server NIPC email to NERC	All NERC and electric power entities

The NIPC and information recipients recognize that each organization receiving warning notifications may incur expenses or possibly suffer some degraded system performance temporarily by raising security levels. Consequently, and to assure that such periods of heightened security are kept to the minimum commensurate with the situation, the NIPC will endeavor to establish and include a time horizon in each warning message.

The NIPC and information recipients also recognize that the information referenced in this document is submitted and disseminated in good faith, but otherwise is without warranty.

In addition to warning products noted above, the NIPC periodically will make available analytic products (e.g., Cyber Notes) to electric power entities using various means of communications including InfraGard and NIPC's public web-server.

4. PROSPECTIVE PARTICIPANTS:

Government and industry entities wishing to participate in the NIPC IAW program for electric power may submit requests to do so to NERC by telephone (609-452-8060), FAX (609-452-9550), or email (cipdata@nerc.com). Recognizing that electric power incidents of national significance are the primary focus of this process, applications to participate in this program will be reviewed by NERC for authentication purposes.

5. SOP UPDATE AND CHANGE:

The NIPC IAW Program Manager is responsible for maintaining this SOP and has processes in place for regular updates as needed. NIPC will consider SOP changes recommended by the NERC Critical Infrastructure Protection Working Group or others who become aware of changes needed or who wish to make recommendations for improvements. Recommendations for change should be made by notifying the NIPC Watch & Warning Unit (ATTN: IDSU Unit Chief) by telephone (202-323-3204, -3205, -3206), FAX (202-323-2079, -2082), or email (nipc.watch@fbi.gov).

Draft Specification
Indications, Analysis &Warning (IAW)
Criteria & Thresholds for Reporting Incidents
Affecting Electric Power

Electric utilities and other entities involved in the generation, transmission, control, power marketing and distribution of power are requested to report voluntarily to the NIPC data on incidents that meet the criteria specified in the following pages[1]. The data to be reported is specific to each event criterion as identified under the major categories of 'Physical[2]' and 'Threats.' Reporting will be made in accordance with the SOP Guidelines and the time frames should be met when possible. In the event specified reporting times cannot be met, then reporting will be made when the criteria and thresholds have been met using a timeframe that is reasonable and practical. Cyber attacks and threats, physical attacks and threats, and combinations thereof fall within the range of activities of malicious origin, or unknown and potentially malicious origin, for which this IAW program is developed. The data requested to be reported is either readily available system operational data or data that is available through a power entity's physical security and information security operations[3]. Moreover, these IAW data reporting requests are not intended to duplicate or substitute for information required by law to be reported to DOE.

PHYSICAL EVENTS

The purpose of IAW in this category is to provide data that enables NIPC to warn others, if appropriate, of attacks that are imminent or underway. Reporting of events meeting the guidelines in this attachment is strongly encouraged when the cause is **known** or **suspected to be** of malicious origin. Reporting of events where the cause is uncertain or unknown is also strongly encouraged (i.e., still uncertain or unknown beyond the time periods designated by the criteria herein). Reporting is not necessary if it is considered highly probable that the cause is **NOT** of malicious origin, or until such time that a reportable cause is established.

1.a. Event Criterion: Loss of generation by a utility or generator supply entity.

[1] No procedure established by this Standard supercedes existing mechanisms and channels for reporting company incident data to the FBI, RCMP or other law enforcement agencies.
[2] That is, produces observable consequences (e.g., service outage, degraded operation).
[3] It is recognized that intrusion detection, detection of malicious code, and other computer security violation detection tools for detection of malicious Cyber activities are currently in the process of development and deployment within the electric power infrastructure as well as in other critical infrastructures.

1.b. Event Threshold: Loss of ≥ 500 MW generation in the host region for 30 minutes or longer due to malicious or unknown causes.

2.a. Event Criterion*:* Loss of High Voltage (HV) substations or ac or dc transmission or tie lines.
2.b. Event Threshold*:* Any power disruption from malicious or unknown causes lasting 60 minutes or longer[4] at HV substations (≥ 230kV) or on HV transmission or tie lines (≥ 230kV), unless the provider considers a facility at a lower voltage level to be essential for system operation.

3.a. Event Criterion*:* Loss of distribution substations or lines serving facilities at federal and state levels performing national security or emergency preparedness (NS/EP) functions.[5]
3.b. Event Threshold*:* Any power disruption at distribution substations or distribution lines directly serving national security or emergency preparedness (NS/EP) facilities. Due to the sensitive nature of the NS/EP customers served by these locations, all power disruptions affecting them and lasting 5 minutes or longer should be reported whether due to malicious causes, or not.

4.a. Event Criterion: Loss of distribution substations or lines serving electric system operation facilities[6] (e.g., control area operations, Security Coordinators, ISOs).
4.b. Event Threshold: Any power disruption from malicious or unknown causes at distribution substations or distribution lines directly serving power system operation facilities and lasting 30 minutes or longer.

5.a. Event Criterion: Unanticipated loss of major load center.
5.b. Event Threshold: Any loss of firm load (demand) from malicious or unknown causes lasting for ≥30 minutes at a major load center (i.e., ≥200MW), or amounting to ≥50% loss of firm load served prior to the time of the loss.

6.a. Event Criterion: Loss of critical telecommunications for functions described in events 1-5 (above) as being essential to system operation (including radio, wireline and wireless-both voice and data).
6.b. Event Threshold: Significant loss or degradation of critical telecommunications (including telemetry) from malicious or unknown causes that impairs the ability of the system to perform essential functions associated with control (e.g., SCADA, EMS,

[4] Once a disruption occurs lasting 60 minutes or longer and meeting the criteria associated with this threshold, reporting is to be made within the ensuing 60 minutes. However, the 60 minute reporting period may be extended due to special circumstances, such as the need to investigate incidents involving transmission facilities that are not readily accessible. Reporting entities still should attempt to meet the 60 minute guideline, if possible.
[5] A categorical list of strategically significant national security and emergency preparedness facilities listed by state and geographical location will be provided by NIPC.
[6] A categorical list of facilities by state engaged in power system operation functions (e.g., control area operations, Security Coordinators, ISOs) will be provided by the North American Electric Reliability Council (NERC).

Control Center, RTUs, OASIS, transaction tagging) or other critical operational or maintenance functions.

7.a. Event Criterion: Loss or degraded ability to control operations over a portion of the power grid.
7.b. Event Threshold*:* Any loss or degradation of essential control functions from malicious or unknown causes lasting 30 minutes or longer at several transmission substations, or repeated losses at a single transmission substation, associated with a portion of the grid serving 100,000 customers or more.

8.a. Event Criterion: Loss or degraded market functionality.
8.b. Event Threshold: Loss or degraded market functionality from malicious or unknown causes, or of information systems (e.g., OASIS, iDC, tagging, transaction schedules) or telecommunications systems (e.g., Internet) critical to that functionality, including national or regional power markets; day-ahead, hour-ahead, or real-time markets; commodity**,** spot or futures markets having a financial impact greater than $1 million.

9.a. Event Criterion: Anomalous or Non-Characteristic System Behavior
9.b. Event Threshold: Any anomalous behavior—in the judgement of NERC Security Coordinators—involving generation, bulk power transmission, control of bulk power, or in wide area networks serving the bulk power system lasting 30 minutes or longer.

THREAT EVENTS

The purpose of IAW in this category is to provide data that enables NIPC to disseminate advance warnings (‘strategic warning’).

10.a. Event Criterion*:* Announced and credible threats that, in the judgement of the reporting organization, potentially could affect the reliability of the electric system or the ability of the organization to conduct business or fulfill its mission.
10.b. Event Threshold*:* Any credible explicit threat conveyed by any means.

11.a. Event Criterion*:* Intelligence gathering: physical surveillance.
11.b. Event Threshold*:* Any unauthorized or suspicious physical, photographic, or electronic surveillance (e.g., passive microwave control signal monitoring, infra red imaging) being conducted on the physical plant comprising an electric power system that, in the judgement of the operator, potentially could affect the reliability of the electric system or the ability of the organization to conduct business or fulfill its mission..

12.a. Event Criterion: Intelligence gathering and operations: Cyber surveillance, intrusions, attacks.

12.b. Event Threshold: Report within 1 hour after detection any unauthorized, highly focused and concerted Cyber attempts against, or intrusions into[7], critical operational power systems that potentially could affect the reliability of the electric system or the ability of the organization to conduct business or fulfill its mission and identify the target systems, impact on those systems, and external network addresses or other identifier of the apparent source of the attempts or intrusions.

13.a. Event Criterion: Intelligence gathering: Social Engineering.
13.b. Event Threshold: Any outside or unauthorized inside attempts to extract sensitive or proprietary information from employees that, in the judgement of management, could aid in planning or executing Cyber intrusion or physical attack.

14.a. Event Criterion*:* Security breaches affecting computer systems, networks, communications, and/or data storage systems that potentially could affect the reliability of the electric system or the ability of the organization to conduct business or fulfill its mission.
14.b. Event Threshold*:* Detection of breach of security in any one, or combination thereof, of the following security components that potentially could affect the reliability of the electric system or the ability of the organization to conduct business or fulfill its mission: information availability (through denial-of-service), corporate network boundary, access control, authentication, confidentiality, data integrity, and non-repudiation.

15.a. Event Criterion*:* Planting or Pre-Positioning of Malicious Code/Exploit Tools
15.b. Event Thresholds*:* Activities such as: unauthorized downloading, transferring, planting, or pre-positioning malicious code (including viruses) or computer/network exploit tools that potentially could affect the reliability of the electric system or the ability of the organization to conduct business or fulfill its mission.

[7] Examples of focused unauthorized attempts or attacks may include Cyber tools repeatedly aimed at specific hosts, servers, sub-nets, or selective network address ranges with the objective of gathering intelligence, penetration, or denial-of-service.

Rev 1.0; June 2000

Attachment B

Incident Report Form
National Infrastructure Protection Center (NIPC)

Tel: **202-323-3204, -3205, -3206**
FAX: **202-323-2079, -2082**
email: **nipc.watch@fbi.gov**
secure InfraGard web-server

Instructions for filing:

Stage 1 Reports--due within 60 minutes after an incident occurs meeting one of the 15 event criteria

Complete Section 1 only

Stage 2 Reports--due within 4-6 hours after Stage 1 Report

Complete Section 2 for Physical Incidents

Complete Section 3 for Cyber Incidents

Stage 3 Reports--due within 60 days after incident occurs
(or on a schedule set by filing entity)

Supplement information on Sections 2 & 3 as appropriate

Methods for filing:

Reports may be completed and filed using InfraGard secure web-server

OR

Reports may be completed by using this EXCEL form and then forwarded by email or FAX to the numbers shown above

Rev 1.0; June 2000 — Attachment B

>Section 1: Electric Power<

Reporting Stage:	Stage 1	Stage 2	Stage 3
Original			
Revision			

NIPC File ID _____ Originator's Security Designation: _____ (if any)

"This information is provided pursuant to NIPC SOP; Electric Power IAW Activities; dated May 2000"

1. Name of Company Filing Report:

(check all that apply)

Generation Company	Operator	Security Coordinator	Transmission/ Distribution Provider	PSE	Other

2. NERC Region Hosting Company Filing Report: (check one)

ECAR	ERCOT	FRCC	MAAC	MAIN
MAPP	NPCC	SERC	SWP	WSCC

3. Contact Data for Person Filing Report:

Name	Telephone #	FAX#	eMail	eMail

4. Event Criteria Satisfied: (Check all that apply)

1-Loss of Generation	2-Loss HV Transmission	3-Loss of Distribution	4-Loss of Distribution	5-Loss of Load Center
6-Loss of Telecom for System Ops	7-Loss of or Degraded System Control	8-Loss or Degraded Market Functionality	9-Anomalous/ Non-Characteristic System Behavior	10-Announced & Credible Threats
11-Intelligence Gathering: Physical Surveillance	12-Intelligence Gathering: Cyber Surveillance/ Operations	13-Intelligence Gathering: Social Engineering	14-Security Breaches Affecting IT	15-Planting/ Pre-Positioning Malicious Code

(If any boxes in the shaded area [above] are checked, be sure to complete Section 3.)

[In any case, fill out the remaining portion of Section 1 and 2, as appropriate.]

Tel: **202-323-3204, -3205, -3206**
FAX: **202-323-2079, -2082**
email: **nipc.watch@fbi.gov**
secure web-server

Rev 1.0; June 2000 Attachment B

Section 1 (Stage 1) Report (Cont'd)

5. Critical Dates/Times: (indicate time zone) _____

Filing	Receipt of Threat	Onset of Outage	Onset; Degraded System Performance	Other
☐	☐	☐	☐	☐

6. Threat/Incident Directed At: (check all that apply)

Own System	Other System	(Name System)
☐	☐	_____

7. Cause of Outage/System Degradation: (check one)

Malicious	Unknown	Non-Malicious
☐	☐	☐

(Skip to Section 2)

8. Type of Incident: (check all that apply)

Operational	Cyber	Unknown
☐	☐	☐
(Complete Section 2)	**(Complete Sections 2 & 3)**	**(Complete Section 2)**

ADDITIONAL COMMENTS

Tel: **202-323-3204, -3205, -3206**
FAX: **202-323-2079, -2082**
email: **nipc.watch@fbi.gov**
secure web-server

Rev 1.0; June 2000 Attachment B

Section 2: Operational Information

NIPC File ID#_____

(Check All That Apply)

Originator's Security Designation: _____ (if any)	**Filing For:**	**Stage 2**	**Stage 3**
	Original		
	Revision		

1. Location of Initiating Event:

Affected Component: (specify)	**Lat/Long** (if known)	**Nearest City**	**Host State(s)**
	N		
	W		

2. Location of Area(s) Affected:

State(s)	**NERC Regions**	**Nearest Landmark**
		(City/County)

3-Incident Impacts: (Fill in All)

Actual (Check One)	**Potential**	**Duration: (Estimate)** (Check One)		**MWs Lost** (Check One)	
		(Hrs.)		100	
			(enter no.)		(enter no.)
		(Days)		1000	

4-Cross-Sector Inputs Affected

(check all that apply)

Telco	**Water Mgmt**	**Trans.**	**Banking/ Finance**	**Petroleum**	**Gas**	**Other**

Please Enter Additional Details for Physical Events

Tel: **202-323-3204, -3205, -3206**

FAX: **202-323-2079, -2082**

email: **nipc.watch@fbi.gov**

secure web-server

Rev 1.0; June 2000 Attachment B

Section 3: Cyber Incident Data

NIPC File ID#_____ **(Check All That Apply)**

Originator's Security Designation: _____ (if any)	**Filing For:**	**Stage 2**	**Stage 3**
	Original		
	Revision		

Impact Category: (add rows if necessary) (fill in all that apply)	**Identify Probe/ Exploit by Name (if known):** (if unknown, enter 'Unknown Tool')	**Date/Time of Occurrence:** (enter time zone)	**Network Address/ Source Name:** (only if external) (#hits/period)	**Target System Name/ Platform:**	**Target System Function Within Power Operations:** (enter all that apply) EMS SCADA Subst OTHER	**Impact on Target System & Power Operations: (Actual)**	**Impact on Target System & Power Operations: (Potential)**
1- Obtains System/User Information through random Probes/Scans/Sniffers, etc.							

Tel: **202-323-3204, -3205, -3206**

FAX: **202-323-2079, -2082**

email: **nipc.watch@fbi.gov**

secure web-server

Rev 1.0; June 2000	Section 3: Cyber Incident Data (Cont'd)					Attachment B	
	Probe	**Date/Time**	**Network Address**	**Target System**	**System Function**	**Impact (Actual)**	**Impact (Potential)**
2-Obtains Root, User, or Mixed Access							
3-Causes Denial-of-Service							
4-Theft-of-Service/ Theft-of-Information							
5-Removal/ Modification/ Corruption of System, User Data							
		Tel: **202-323-3204, -3205, -3206**					
		FAX: **202-323-2079, -2082**					
		email: **nipc.watch@fbi.gov**					
		secure web-server					

Rev 1.0; June 2000	ection 3: Cyber Incident Data (Cont'd)					Attachment B	
	Probe	**Date/Time**	**Network Address**	**Target System**	**System Function**	**Impact (Actual)**	**Impact (Potential)**
6-System Mod/Augmntn (malicious code insert etc.)							
7-Identifies Critical Sys Supporting Power Ops							
		Tel: **202-323-3204, -3205, -3206**					
		FAX: **202-323-2079, -2082**					
		email: **nipc.watch@fbi.gov**					
		secure web-server					