RECLAMATION

Managing Water in the West

Facilities Instructions, Standards, and Techniques
Volume 6-3

Unexpected Event Reporting

U.S. Department of the Interior
Bureau of Reclamation
Denver, Colorado

August 2011

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
8-11-2011

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
Published August 19, 2011
Effective September 19, 2011 until superseded

4. TITLE AND SUBTITLE
FIST 6-3, Unexpected Event Reporting

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Martin Bauer, Nick Bunting, Jeffery Hoffman, Rick Jackson, Terry Kent, Toni Linenberger, Steve Melavic, and Max Spiker,

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Bureau of Reclamation
Denver Federal Center
P.O. Box 25007
Denver CO 80225-0007

8. PERFORMING ORGANIZATION REPORT NUMBER
FIST 6-3

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Power Resources Office, Technical Resources
Bureau of Reclamation
Mail Code 86-61600
PO Box 25007
Denver CO 80225-0007

10. SPONSOR/MONITOR'S ACRONYM(S)
PRO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Available from the National Technical Information Service, Operations Division, 5285 Port Royal Road, Springfield, Virginia 22161

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Bureau of Reclamation operates and maintains 53 hydroelectric powerplants and many switchyards, pumping plants, and associated facilities that are important to electric power and water delivery systems. These facilities house complex electrical and mechanical equipment; protective relays and associated circuits play an essential role in protecting this equipment as well as the electric power system. Improving the reliability of this equipment is facilitated by analyzing the event when that equipment operates and ensuring that the operation is correct to prevent the recurring events. This document defines Reclamation practices for documenting unexpected events at Reclamation power facilities.

15. SUBJECT TERMS
Unexpected event reporting

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Martin Bauer
U	U	U	U		**19b. TELEPHONE NUMBER** *(include area code)* 303-445-2901

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. 239-18

United States Department of the Interior

BUREAU OF RECLAMATION
P.O. Box 25007
Denver, Colorado 80225-0007

AUGUST 16 2011

IN REPLY REFER TO:
86-61600
PRJ-19.00

MEMORANDUM

To: Regional Directors
Attn: PN-1000, MP-100, LC-1000, UC-100, GP-1000

From: Michael R. Gabaldon
Director, Technical Resources

Subject: Revised Facilities Instructions, Standards, and Techniques (FIST) Volume 6-3, "Unexpected Event Reporting" (FIST 6-3)

Attached to this memorandum is the revised FIST Volume 6-3, "Unexpected Event Reporting."

The Unexpected Event Reporting program in FIST 6-3 replaces the Equipment Trouble Reporting Program and the Incident Reporting Program covered under FIST Volume 1-2 "Operations Improvement Program." The Unexpected Event Reporting program has been in development with representatives from each of the regions over the past two years. The program objective is to provide a process to increase the reliability at all Bureau of Reclamation facilities with power features. In addition, this program will also be instrumental in providing processes and documentation in support of compliance with North American Electric Reliability Corporation reliability standards. This FIST 6-3 has undergone extensive review and modification. FIST 6-3 incorporates Reclamation standard practices text highlighted in bold and brackets consistent with the Temporary Reclamation Manual Release FAC TRMR- 32 "Power Facilities Technical Documents." The effective date for FIST Volume 6-3 is September 19, 2011.

FIST volumes may be accessed via the intranet at http://intra.usbr.gov by selecting "Power O&M" from the Quicklist, or via the internet at http://www.usbr.gov/power/data/fist_pub.html. Hard copies are available from the Power Resources Office, (PRO) 86-61600 by contacting PRO at 303-445-2922.

Attachment

cc: 84-21000 (Muller, Hoffman), 84-21131 (Ehler), 84-43000 (Meredith),
84-45000 (Schuster, Linenberger), 84-50000 (Gonzales), 84-57000 (Herrera, Krause),
86-61000 (McCalman), 86-61600 (Bauer, Jackson, Spiker)
PN-6100 (Kent), CVO-600 (Melavic), GP-2020 (Bunting
(w/att to ea)

Continued on next page.

Continued from previous page.

cc: GCP-1000 (15 copies)
HH-3000 (5 copies)
SRA-1000 (10 copies)
CCA-1000 (6 copies)
PN-3040 (1 copy)
PN-6100 (1 copy)
SCC-100 (10 copies)
NC-100 (20 copies)
KO-100 (1 copy)
CC-100 (15 copies)
LO-100 (2 copies)
MP-160 (1 copy)
MPCO-100 (1 copy)
CVO-600 (12 copies)
PXAO-1000 (6 copies)
YAO-1000 (10 copies)
LC-1000 (1 copy)
LC-4000 (1 copy)
LC-6020 (1 copy)
LC-9000 (4 copies)
LCD-1000 (1 copy)
LCD-1050 (24 copies)
LCD-D10 (4 copies)
LCD-P10 (4 copies)
SCAO-1000 (1 copy)
ALB-100 (1 copy)
FCCD-100 (1 copy)
EB-600 (1 copy)
UC-600 (4 copies)
UC-1010 (1 copy)
PRO-100 (1 copy)
WCG-CDeAngelis (2 copies)
GC-100 (16 copies)
CCI-100 (10 copies)
FG-100 (5 copies)
MT-100 (10 copies)
NK-100 (4 copies)
TX-Trevino (6 copies)
DK-1000 (6 copies)
WY-1000 (25 copies)
EC-1000 (25 copies)
GP-1270 (1 copy)
GP-2020 (3 copies)

Facilities Instructions, Standards, and Techniques
Volume 6-3

Unexpected Event Reporting

Prepared by:

Power Resources Office

U.S. Department of the Interior
Bureau of Reclamation
Denver, Colorado

August 2011

Disclaimer

This written material consists of general information for internal use only by Bureau of Reclamation operations and maintenance staff. Information contained in this document regarding commercial products or firms may not be used for advertising or promotional purposes and is not to be construed as an endorsement or deprecation of any product or firm by the Bureau of Reclamation.

Acronyms and Abbreviations

AGC	Automatic Generation Control
CIO	Chief Information Officer
DOC	Designers Operating Criteria
FIST	Facilities Instructions, Standards, and Techniques
NERC	North American Electric Reliability Corporation
O&M	Operation and Maintenance
PEB	Power Equipment Bulletin
PDF	Portable Document Format created by Adobe Systems
PLC	Programmable Logic Controller
PRO	Power Resources Office
PO&M	Power Operations and Maintenance
RCSIRT	Reclamation Computer Security Incident Response Team
RDO	Reclamation Duty Officer
Reclamation	Bureau of Reclamation
REO	Regional Emergency Official
RESC	Reclamation Enterprise Service Center
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SMIS	Safety Management Information System
SOP	Standing Operating Procedure
SSLE	Security, Safety, and Law Enforcement
WECC	Western Electricity Coordinating Council

Contents

FIGURES

1. Introduction

The Bureau of Reclamation (Reclamation) operates and maintains 53 hydroelectric powerplants and many switchyards, pumping plants, and associated facilities in the 17 Western States. These facilities are critical to the electric power and water delivery systems relied on by many. They contain complex electrical and mechanical equipment that must be kept operational. The analysis of events will increase availability of the facilities. The analysis is only possible by documenting those events. With the documentation, the analysis can result in a meaningful corrective action plans to reduce event recurrence.

Text that appears bold and brackets in this Facilities Instructions, Standards, and Techniques (FIST) volume is considered a Reclamation standard practice. Reclamation standard practices reflect minimum operations and maintenance (O&M) activity levels. Variation from Reclamation standard practices and schedules is acceptable provided that local instructions exist to support the variation. Non Bold text is a suggested practice or explanation. Variation from suggested practices or explanation does not require Local Instructions.

1.1 Purpose and Scope

The purpose of this document is to provide practical guidance to Reclamation staff in evaluating and reporting unexpected events. It is to be used by personnel in the facility, area, regional, and Denver offices to conduct the various levels of unexpected event evaluation and reporting.

[This FIST is applicable at facilities operated and maintained directly by Reclamation staff and can be applied at facilities that are owned by Reclamation but maintained by others. Each region will determine the degree to which the program can be applied to their respective facilities that meet this criteria.]

The Unexpected Event Reporting Program is a structured approach to evaluating and documenting events. This is accomplished by a defined process of event assessment that is tailored in scope and depth to the severity of the event. Foremost, the Unexpected Event Reporting Program is intended to be a learning tool for the betterment of our operations and maintenance programs through self-examination and information sharing. Specific actions include:

- To evaluate unexpected events to determine the causes of the event for the purpose of improving operation, maintenance, construction, and management practices; and emphasizing enhanced safety and health in Reclamation facilities.

- To prevent future occurrences of similar incidents through the dissemination of information, lessons learned, and remedies throughout Reclamation.

1.2 Effective Dates

This FIST will be effective 30 days after the date of publication listed on the cover or as defined in the Local Instructions of the respective facilities.

1.3 Definitions

The following definitions are adopted collectively as a standard for the purposes of this FIST.

Charter

A document commissioning a group of individuals with the authority to conduct specific investigation activities. The document includes specific deadlines, objectives, and assignment of team members and team leader as well as instructions concerning funding and is signed by all team members and the representative of the commissioning office.

Corrective Actions

Documented planned actions and timelines for completion to prevent recurrence of events.

Corrective Action Plans

A document that compiles the Corrective Actions for a specific event.

Cyber Asset

An electronic device which is programmable over a serial or IP addressable port, or a communication network device.

Incident

Any unexpected event that is classified as Significant or Severe.

Investigation Team

The staff assigned to collect and review data involved with the event, conduct analysis of the data and develop findings of the cause of the event and identify contributing factors. Except where specifically indicated otherwise, the Investigative Team referred to throughout this FIST is one assigned to examine the operational issues and characteristics of the unexpected event (as distinct from the law enforcement or criminal issues or characteristics.)

Minor Event

The classification of events which have the following attributes:

1) Any unscheduled change in water operations that is not the result of weather.

2) Any Unexpected Event of any component of any power or auxiliary equipment (including gates or valves) that can effect generation or water equipment that is not being commissioned or tested. Relay operations off line or on-line.

3) Any unplanned loss of Supervisory Control and Data Acquisition (SCADA) systems, communications systems, or remote control components.

Misoperation

Any Unexpected Event that involves any device associated with the power or water control or protection that did not operate as expected or whose proper operation in an Unexpected Event could not be validated. This also includes electronic devices or systems associated with Programmable Logic Controller (PLC) or Remote Terminal Unit (RTU) functions.

Restoration Team

The staff (one or more) dispatched or assigned to respond to the event to restore the equipment or facility to safe working condition.

Severe Event

The problem is not contained within one facility and spreads to other facilities, or multiple systems are damaged in a facility. This generally is when a series of events occur, and these events affect more than one facility or the damage involves more than one system in a powerplant and will require a long time to repair. This does not include events when one protection system, i.e., breaker failure, trips multiple powerplants. An event would be considered a potential environmental impact when something goes wrong and fish are possibly stranded because the river level dropped. The classification of a severe event would have the following attributes:

1) The operation of more than one protective system that causes the loss of generation along with damage to more than one system in the facility associated with generation (such as complete lube oil systems and cooling water system) or property damage.

2) An event that causes other relays to trip in more than one switchyard or powerplant.

3) Any unscheduled change in water operations that results in an uncontrolled release or significant drop in release causing an environmental impact and not the result of weather.

4) Any unexpected event that results in widespread property damage outside of the facility.

5) Failure or misoperation of equipment, including operational error that results in damage to multiple station equipment systems or affects the ability of more than two powerplants to provide or be available to provide generation.

Significant Event

The problem is not contained by one protection system in a powerplant or switchyard. This is generally when a series of events occur within a poweplant or switchyard that affects one or more generators or lines or the damage destroys one facility system and will require a long time to repair. The classification of a significant event would have the following attributes:

1) Any unscheduled change in water operations that results in an unintended release or reduction in flow without potential environmental impact and is not the result of weather.

2) Loss of generation with damage to one station's system.

3) Any unexpected event that results in damage to one station's equipment system (such as complete lube oil systems or cooling water system).

4) Two or more protections systems cause a temporary loss of generation or availability of two or more generating units in one facility. This excludes a single protection system operation that affects multiple facilities or units.

Sponsor

Manager or designated representative of the office organizationally one level higher than the manager of the office organizationally responsible for the equipment or facility involved in the event. The Sponsor could be the Area Manager, Power Manager, or Power Resources Manager, etc., depending on the event or organizational structure. As an example, if the event occurred in the Third Powerplant, the Power Manager for Grand Coulee would be organizationally one level higher than the Plant Manager for the Third Powerplant.

Unexpected Event

With the exception of equipment or systems undergoing commissioning or undergoing testing, an unexpected event is an unanticipated action involving

components or systems[1] related to power generation or water delivery. Examples of unexpected events include:

- The interruption of power transmission
- Causes an unscheduled change in water operations
- Damage to equipment associated with power generation, power transmission, or water operations
- Forced outages
- Relay operations with the unit on or offline
- Events that have an impact to the bulk electric system
- Additional events not listed but as determined by the individual region

1.4 Cross References

In addition to the information provided in this FIST, the following documents contain information concerning incident or unexpected event documentation.

FIST 1-1, Hazardous Energy Control Program, March 2002, section 19.5.3

FIST 1-2, Operations and Maintenance Improvement Program, May 1989 (errata needed)

FIST 1-3, Reports and Records, December 1989 (errata needed)

FIST 1-11, Conduct of Power Operations, December 2002, sections 11, 12, and 17.3

FIST 1-12, Abnormal Operations Generic Technical Guidelines for Power Stations, March 2003, section 2.7

FIST 3-30, Transformer Maintenance, October 2000, section 4.4.4

FIST 3-32, Transformer Fire Protection, January 2005, section 16

---

[1] Examples of the components or systems of concern that affect the ability to deliver water, generate power, transmit power, or would render that equipment inoperable include:

- Data and voice communication systems relating to the operation of gates and/or AGC in power plants, including data telemetry required by the Transmission Operator.
- Incorrect operation or failure to operate when called for, of gates or valves that are used to release or control the flow of water in conveyance systems.
- Pumps and generators
- Associated primary power system components like main unit breakers and transformers, stations service breakers, and transformers whose failure or inoperability prevent the operation of generators and pumps.

FIST 4-2, Power O&M Codes for ADP, sections 2.1 to 2.5 (errata needed)

FIST 5-9, Management and Safe Handling Procedures for Sulfur Hexafluoride (SF6) Gas, March 2004, section 11

FIST 6-1, Management of Power Facilities, March 2003 (errata needed)

FIST 6-2, Conduct of Power Maintenance, March 2006, sections 5.9 and 21

SLE 07-01, Emergency Notification System, September 2009

2. Coordination with Other Investigations

The procedures in this FIST are not intended to replace existing reporting through the U.S. Department of the Interior, Safety Management Information Systems (SMIS), Security, Safety and Law Enforcement (SSLE), or North American Electric Reliability Council (NERC). The procedures in this FIST may run in parallel with those reporting programs. In some cases, there may be an overlap in the incident investigation with other programs and needs to be coordinated between the responsible offices. In cases where the Sponsor is determined through a process outside of this FIST, such as a safety investigation or a criminal investigation, the Restoration Team and Investigation Team may provide technical analysis in support of the related investigation. Corrective Action Plans for technical issues related to facility operations and maintenance uncovered through a safety investigation will be developed following the processes in this FIST.

3. Event Documentation

The processes associated with documenting unexpected events quickly becomes complicated when considering the various entities involved in reviewing and analyzing the data associated with the event. A two-page flowchart is provided to provide an overview of the processes. These two pages reflect the activities from when the event is reported to the final notification (see figures 1 and 2). A second flowchart is provided that focuses on the completion of event documentation. Each page of the flow chart represents each page of the event documentation. To better provide a road map for documentation, figures 1–3 depict the activities associated with Unexpected Event documentation. This diagram does not define programmatic responsibility for the activities.

4. General Procedures

Nothing in this section will have bold text. Please refer to the specific sections for areas that are considered a Reclamation standard practice.

To better help in following the procedures described below, please reference the flow charts at the end of this section. Once an Unexpected Event occurs, the preliminary information must be recorded. All Unexpected Events are reported to the Operations Office with operational jurisdiction over the facility. This report includes the name of the facility, equipment involved, the time and date of the event, and any additional facility or equipment involved. The report also should indicate if the Unexpected Event is a suspected nuisance event. The event is numbered and reported as part of the Suspected Sabotage Reporting Procedure. Each event is classified as Minor, Significant, or Severe. Based on this classification, Restoration Teams are dispatched to the location to start the restoration process.

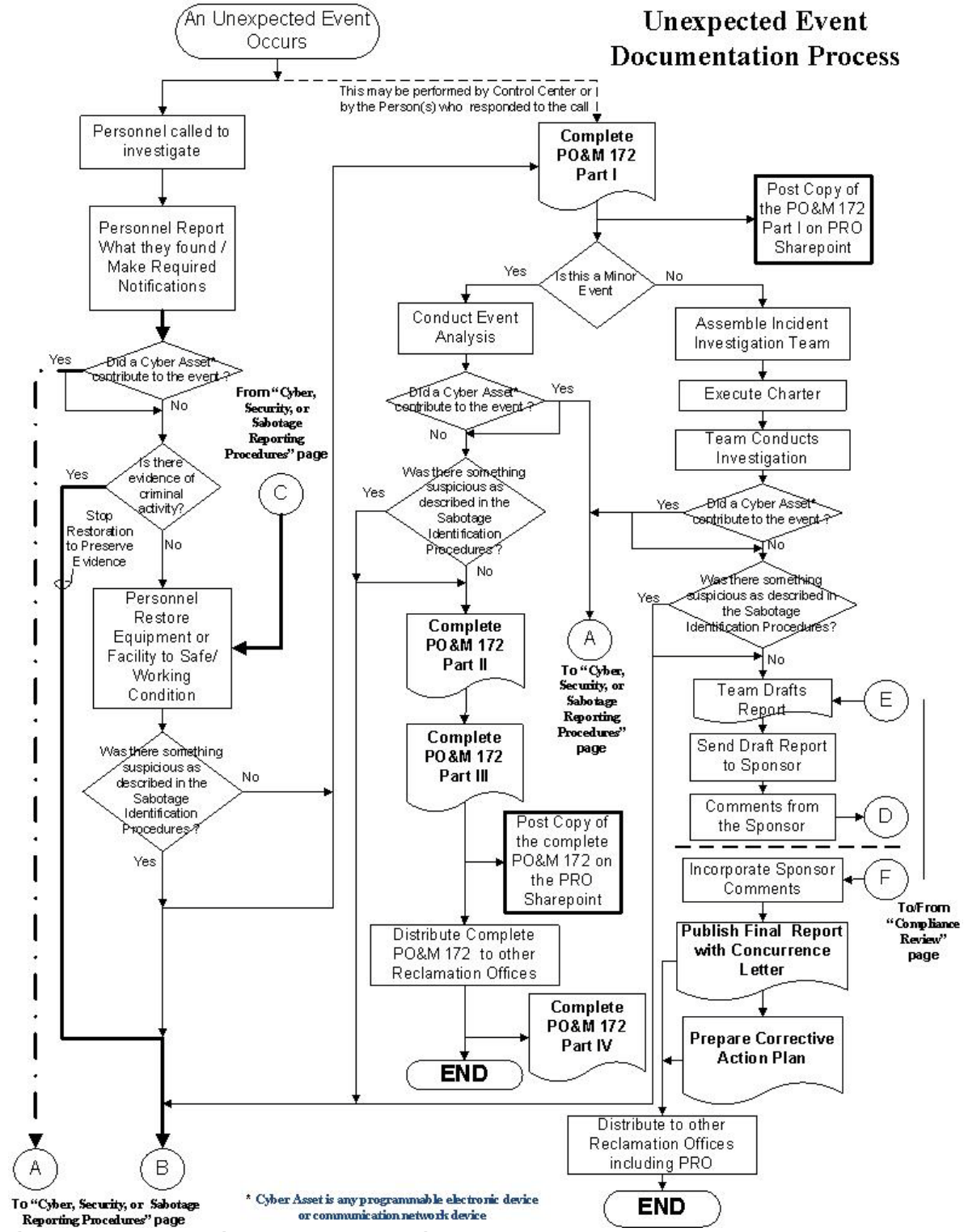

Figure 1. Unexpected Event Documentation Process.

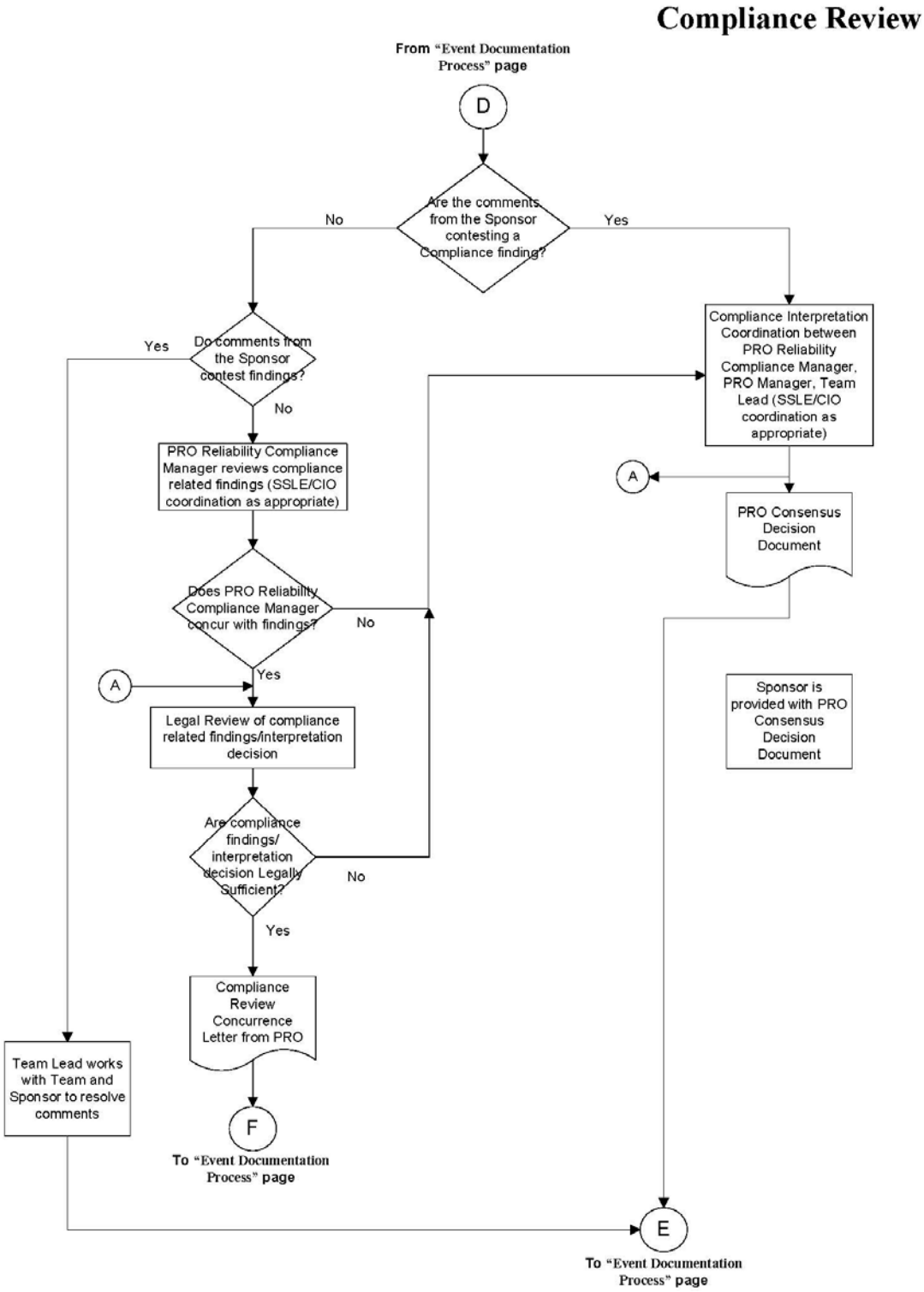

Figure 2. Compliance Review.

CYBER, SECURITY, or SABOTAGE REPORTING PROCEDURES

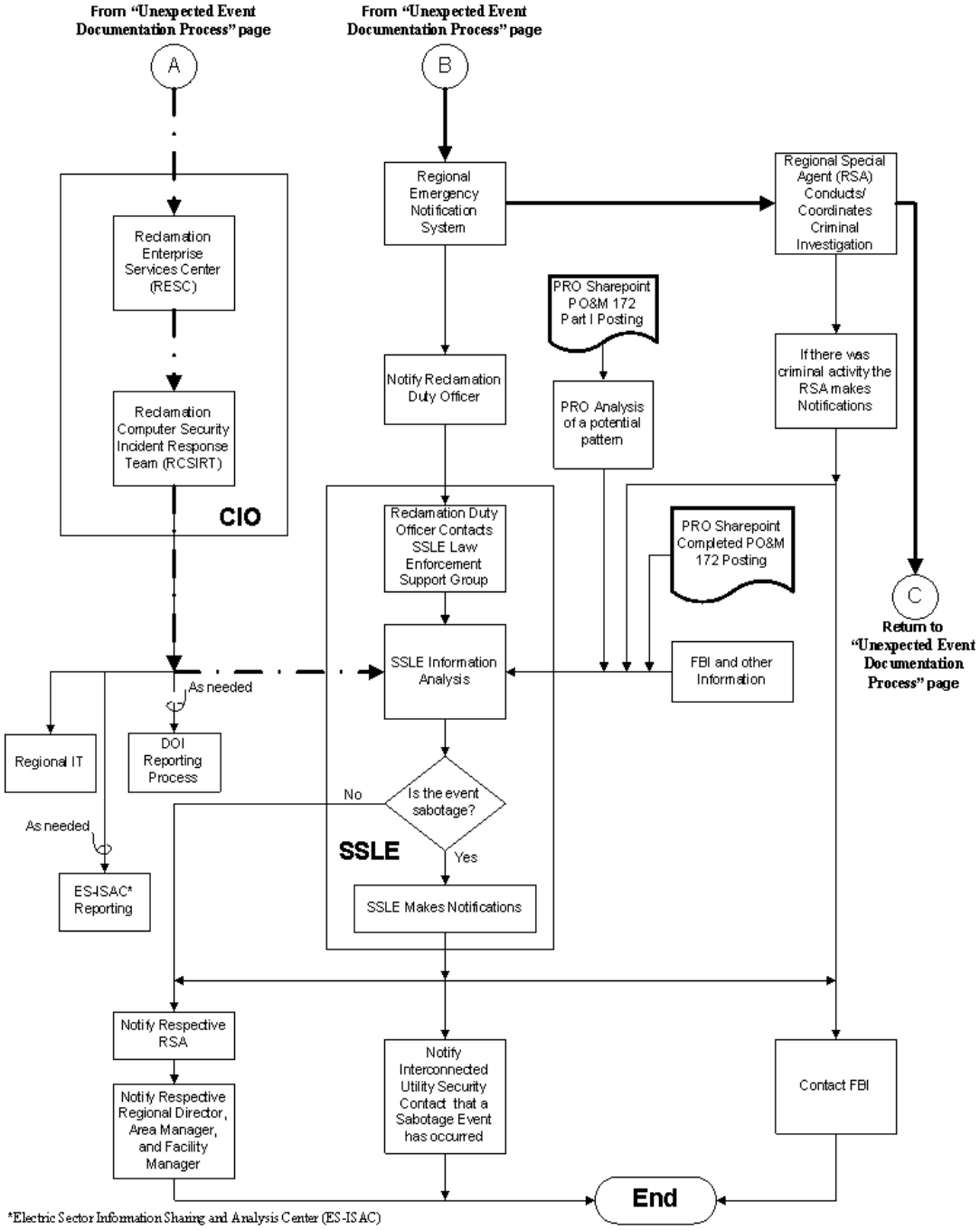

Figure 3. Cyber, Security, and Sabotage Reporting Procedures.

Flow Chart for Completing a PO&M 172 Form

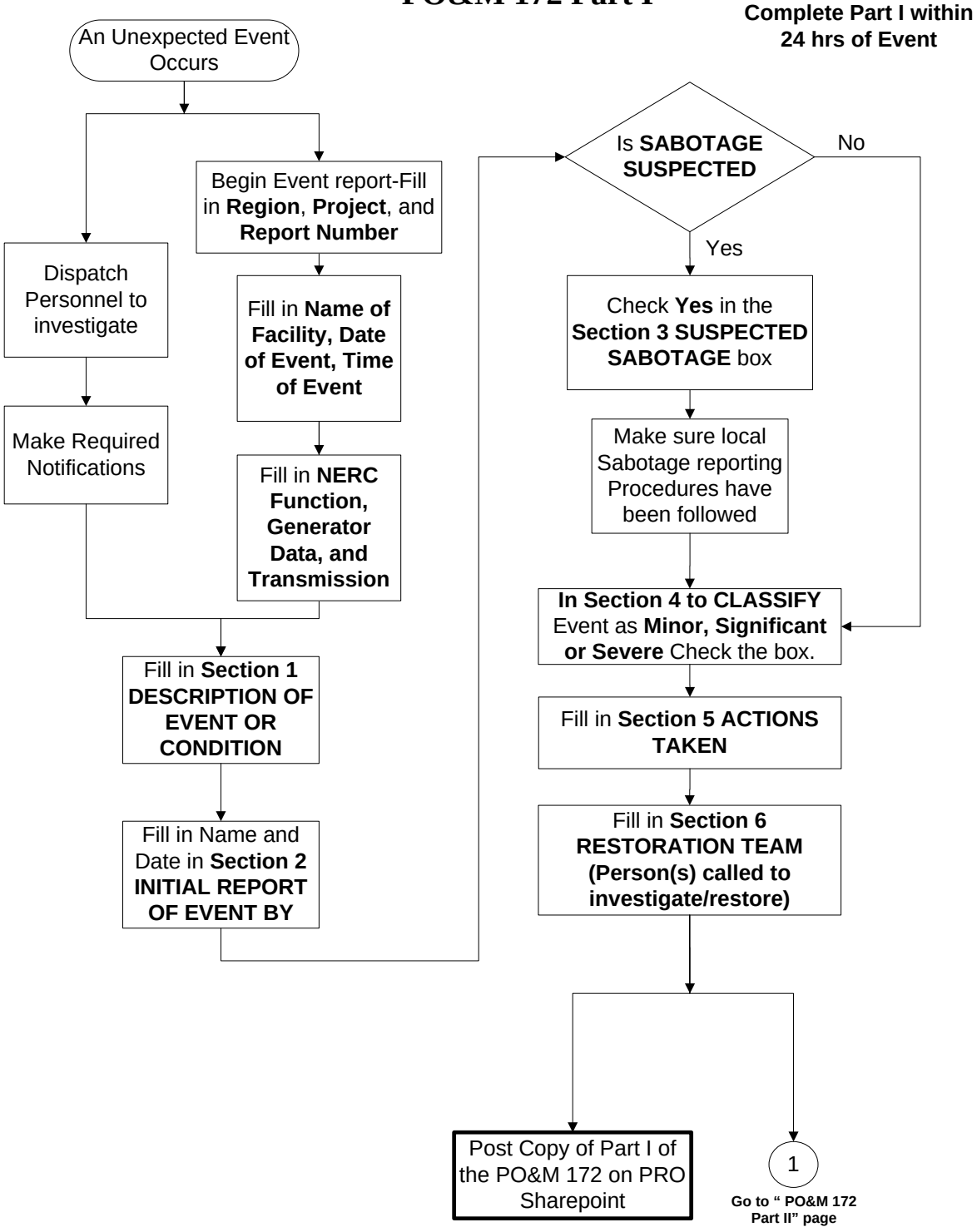

Figure 4. Event Documentation – Filling Out Part I of PO&M 172.

Flow Chart for Completing a PO&M 172 Form (con't)

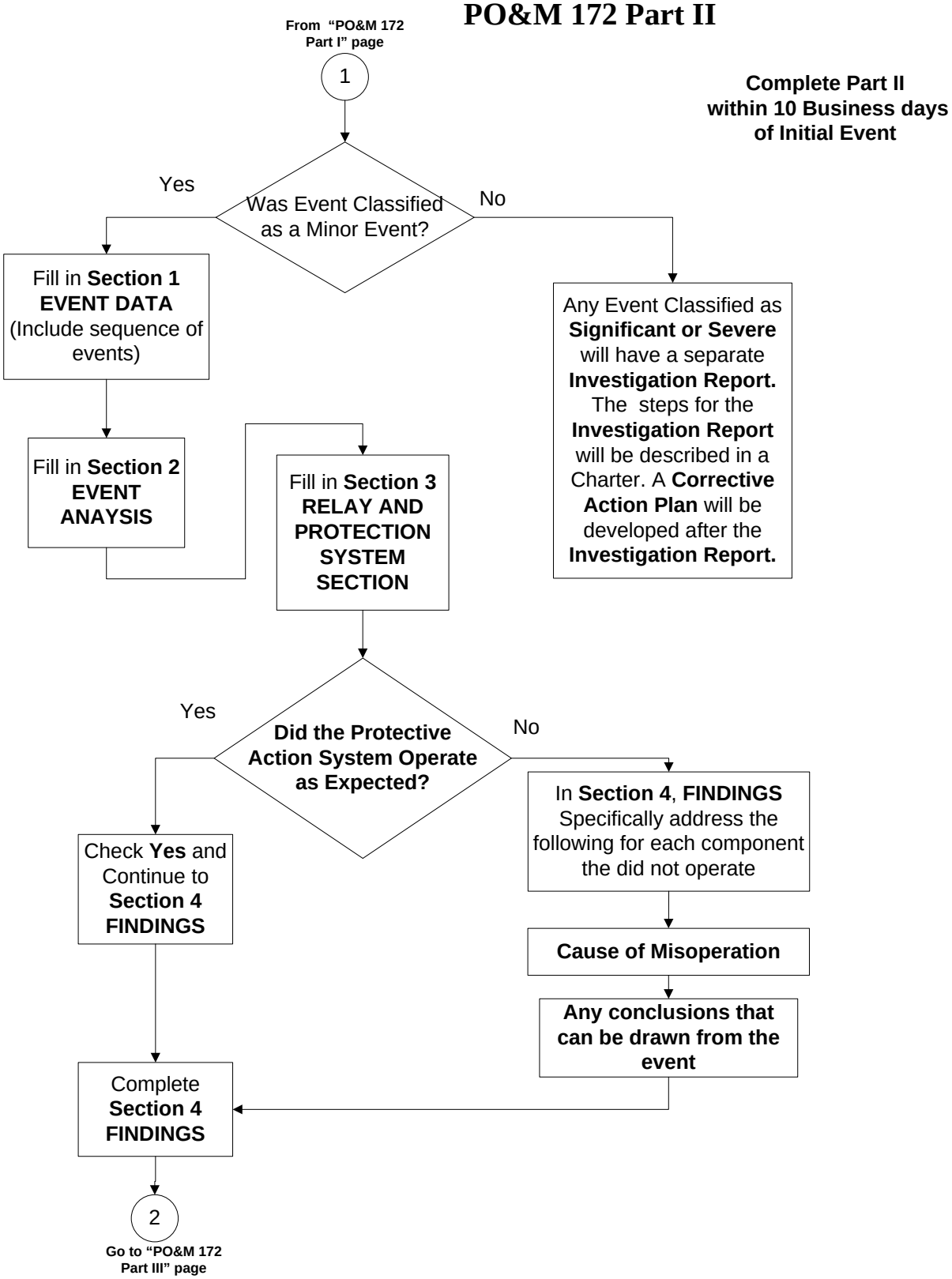

Figure 5. Event Documentation – Filling Out Part II of PO&M 172 (continued).

Flow Chart for Completing a PO&M 172 Form (con't)

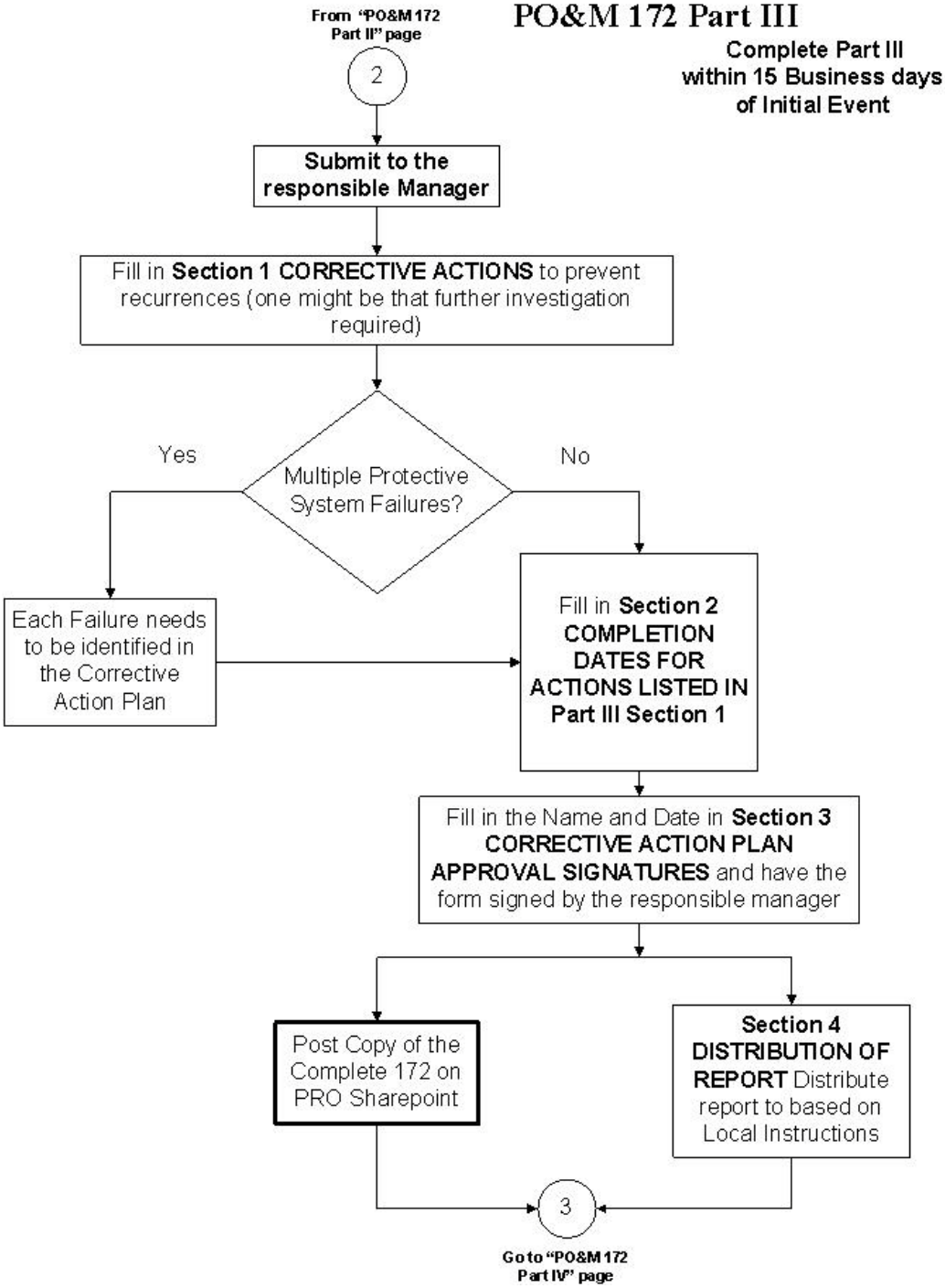

Figure 6. Event Documentation – Filling Out Part III of PO&M 172 (continued).

Flow Chart for Completing a PO&M 172 Form (con't)

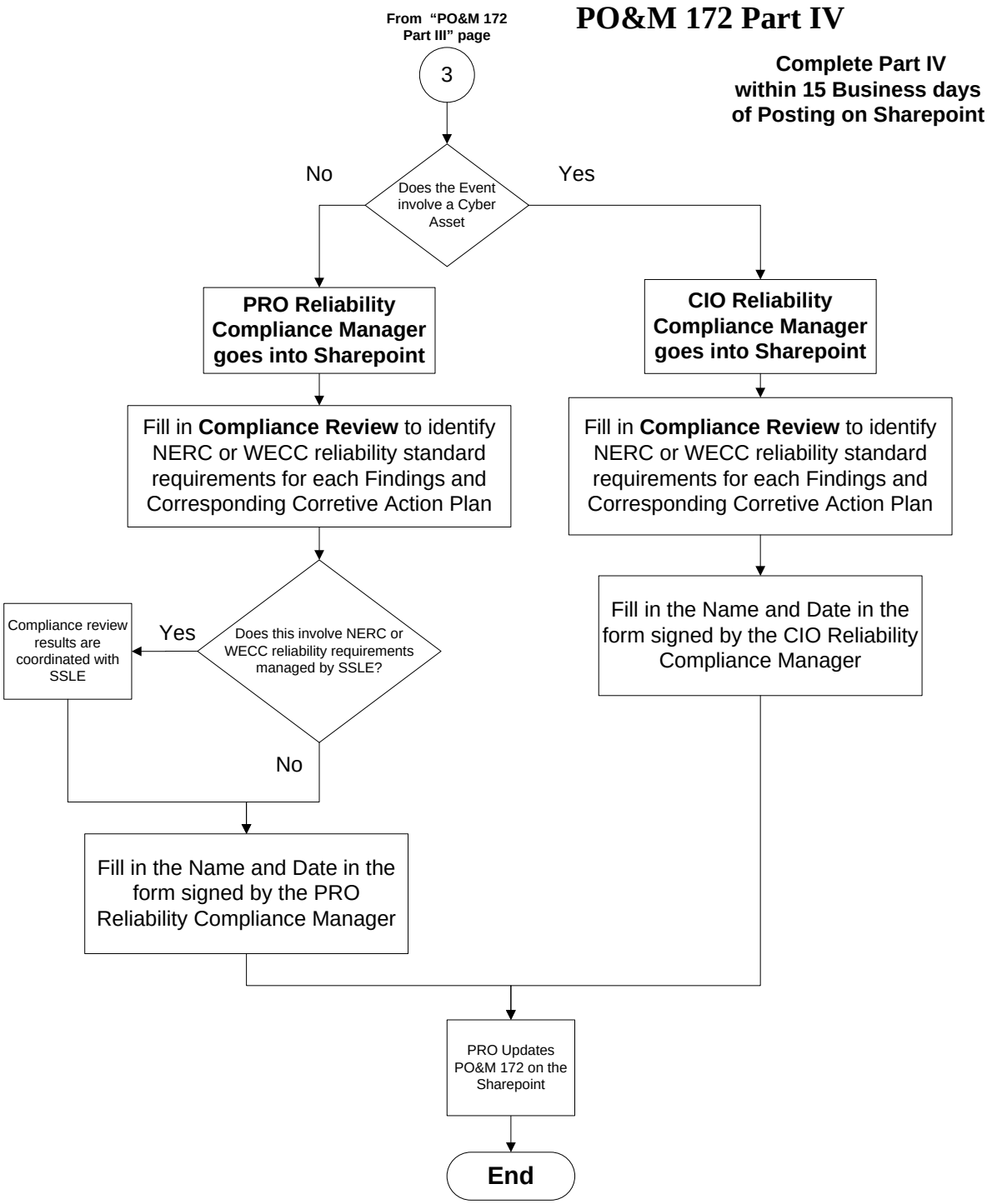

Figure 7. Event Documentation – Filling Out Part IV of PO&M 172 (continued).

In the case of Minor Events, the Restoration Team, which may be comprised of one person to as many additional team members as needed to restore the equipment, will collect, analyze, and document what happened. For the most part, equipment will be restored very rapidly by the Restoration Team. Information that was gathered during the restoration needs to be written down. This information is recorded on the PO&M 172 form (see appendix A) and provided to the manager responsible, who then reviews the information and develops a Corrective Action Plan to prevent recurrence. The Corrective Action Plan is added to the Event Report and submitted to the Area Office Manager. Dissemination of the Event Report does not have to include the Corrective Action Plan.

In the case of Significant Events, the Restoration Team's focus is to restore the equipment and systems in the facility. Information gathered during the restoration needs to be given the Investigation Team. An Investigation Team is assigned by a Sponsor to conduct event analysis through using a Charter (see appendix B). The Investigation Team collects and analyzes data to explain what happened. This information, which includes all the collected data, is assembled in a report. The report is forwarded to the managing office who adds a Corrective Action Plan to the end of the report. This final version is submitted to the Regional Director. The report is disseminated by the region to the respective area offices with power facilities and interconnected utilities, as appropriate.

Severe Events follow a similar process as Significant Event Reporting. The exception is that both the Event Report and the Corrective Action Plan are transmitted separately to the Commissioner. Once received by the Commissioner, the Event Report may be disseminated.

Specific tasks and timelines associated with Unexpected Event Reporting are provided in "Appendix C, Timelines."

5. Event Numbering

[Each Unexpected Event is assigned a unique number corresponding to the year, month, day and the two- or three-digit location designation as defined in FIST 4-2 and the number of events on that day. For multiple events, the last digit will be numbered starting with 1. No specific unit or equipment designation is included in the event numbering.]

For example, an event at Hoover, Nevada side, Unit 2 that occurred on January 2, 2009, would be numbered as 20090102HOV1.

If a second event occurred on January 2, 2009, at Hoover resulting in the loss of SCADA for Unit 3 and Station Service, then the resulting designation would be 20090102HOV2.

Numbering of the event is the responsibility of the Operations Office responsible for the facility and is performed immediately[2] when knowledge of the event occurs and is recorded in the Operations Logbook.

6. Suspected Sabotage Reporting

[If at any time, during restoration, sabotage is suspected, it must be reported via the respective regional emergency notification procedure pursuant to Appendix G. Restoration should be suspended when the sabotage is suspected, absent public safety concerns, so that law enforcement can conduct the appropriate investigation. The suspected sabotage report contains the preliminary information and the unique number assigned to the event as well as an indication if the event is suspected as possible sabotage.] Preliminary information includes information such as elements that tripped the breaker or lockout as would be available from an annunciator, as well as the basis for why the possible sabotage is suspected. The reporting procedures for reporting possible sabotage are attached in "Appendix G, Possible Sabotage Reporting Procedures."

7. Event Classification

[Each Unexpected Event is classified as "Minor," "Significant," or "Severe" using the definitions in this FIST. A table showing how events are classified is provided in "Appendix F, How Events Are Classified." Initial classification is made following the assignment of the unique number by the Operations Office.] The classification may be delayed until additional information concerning the nature of event is relayed back to the Operations Office. Absent additional information, all Unexpected Events are classified as "Minor" by default. Events are generally classified Significant or Severe based on the impact of the Event. Significant Events are generally limited to one facility, such as one of the Coulee powerhouses, with cascading events or damage within that facility. Severe Events involve multiple facilities, such as more than one of the Coulee Powerhouses and the protection systems operations in one plant are cascading and causing the protection systems in the other powerhouses to operate. Another important distinction between Minor Events and Significant and Severe Events is that damage is more widespread. In Minor Events generally only one component is damaged, in Significant Events a complete system is damaged. In Severe Events, the damage is more wide spread and multiple systems are damaged. At this level the notoriety of the event also is considered especially when non agency property is involved. The individual delegated with the responsibility for reviewing the preliminary data will ensure that the event is

[2] Immediate action may be delayed, but no more than 24 hours, if the staff is directly involved in the operations associated with the event.

properly classified. This includes possible changes to the classification based upon additional information discovered during restoration.

8. Restoration Teams

The Restoration Team is dispatched by the Operational Office. [**When responding to Minor Events, the Restoration Team assembles the information needed to ascertain the most suitable means of restoring the equipment or facility to a safe operating condition. In addition, the Restoration Team gathers any additional information needed to analyze the cause of the event. This information is documented by the Restoration Team. Also for Minor Events, the Restoration Team analyzes the information to determine a cause of the event.**

For incidents, the Restoration Team provides the information gathered during restoration to the Investigation Team. The Restoration Team focuses on restoring the equipment or facility to a safe operating condition.]

9. Investigation Team

[The Sponsor will formalize an Investigation Team using a Charter signed by all members of the Investigation Team and the Sponsor.] An example Charter is provided in "Appendix B, Example Charter." The charter also includes instructions to the team concerning to whom the final report will be sent, how many copies, the preferred method of transmittal… etc.

[Investigation Team members are not affiliated with the office responsible for managing the facilities involved in the Significant or Severe Event.

For Significant Events, the Investigations Teams are chartered by the office that is organizationally one level higher than the office responsible for managing the facilities or equipment involved in the event.] The Sponsor should coordinate the investigation with the Regional Power Manager. Investigation Teams may also be chartered for Minor Events as determined by the office responsible for the managing the facilities involved in the event or by the respective Regional Director. [**The Charter for the investigation is approved with team members identified within 5 business days following the classification of the event.]** The costs incurred by the Investigation Team during the course of the investigation are funded by the responsible facilities office responsible involved in the event.

[For Severe Events, the Investigation Teams are commissioned by the Power Resources Office (PRO).] The PRO coordinates the Investigation Teams with the appropriate regional representative. Investigation Teams also may be commissioned by the Office of the Director of Operations. [**The Charter for a**

Severe Events Team is approved with team members identified within 5 business days following the event.

Coordination of the draft report with a Compliance review and resolution of the contested findings is the responsibility of the Investigation Team Lead.]

The process that will help in conducting investigations is provided in "Appendix E, Investigation Process."

10. Event Data

[Event data is collected to establish the sequence of operations] immediately prior to the event as well as all relevant activities during and following the event, including those activities used to restore the facility or equipment to safe operating condition. Event data includes actions taken by specific plant staff; documents associated with the event such as job hazard analysis, switching orders, danger tags, relay settings, sequence of operations or event reports, electronic event data from various forms including multifunction relays, fault data recorders, temperature recorders, SCADA systems; interviews; and Standing Operating Procedures and Designers Operating Criteria excerpts.

Event data collected is preserved in its original state and converted to a suitable PDF format to attach to the Event Report.

11. Event Analysis and Findings

The analysis focus is to determine the cause of the event and to describe in a comprehensive fashion, to the degree possible, why the event occurred. [**The analysis of the event must address actions during the event that were appropriate or expected, including protective relays, switching operations, etc., as well as actions during the event that were not expected, appropriate, or constituted a failure, including protective relays, switching operations, etc.**]

Note: If, at any time during this event analysis, sabotage or criminal activity is detected or suspected, it must be reported via the Sabotage Reporting requirements (reference appendix G) so that law enforcement can conduct a criminal investigation. Law enforcement officials may rely on input from the investigative team or other local staff to support security.

[Analysis also includes calculations that demonstrated proper operation and post event tests conducted to ascertain equipment or system operation.

Information obtained through interviews helps to speed the investigation. This information cannot be used without substantiation through records, equipment operating data, or other forms of documentation. Information obtained from interviews that is not corroborated with evidence is regarded as unsubstantiated and treated accordingly during the analysis.

The findings describe the cause of the event including what actions or operations were appropriate and what actions or operations were not appropriate. Findings draw from the analysis, data, and substantiated information. Findings also describe contributing factors discovered during the event analysis and should be supported with evidence. Organization issues and processes discovered through the investigation and considered material to the cause of the event are included as findings in the Event documentation.

If the event analysis indicates that a Cyber Asset failed to operate properly contributed to the event, the RESC needs to be notified.] This invokes Reclamation's Information Technology Incident Response Procedure. [**Findings that involve reliability compliance must be reviewed to ensure consistency of compliance interpretation as described in Section 13.]**

The analysis of the documentation of events may identify similar events or reoccurring issues within an operating office or across the agency that can be used to help prevent reoccurrences. [**The analysis should look at reports of events for similar occurrences. The analysis should address if the event is similar to previous events and seek to identify underlying apparent causes to prevent recurrence. This analysis would be for Minor, Significant, or Severe Events.]**

During the course of investigating an event, the Investigating Teams may find operating procedures or regulations were violated. Those findings would be included in the report for the appropriate supervisor to consider. Recommendations may or may not be included in the report as requested by the Sponsor. [**Investigation Teams do not make recommendations concerning employee conduct or performance. Investigation Teams do not develop Corrective Action Plans**.]

12. Documentation

Documentation of the event varies with the classification. [**In each case, Part I of the PO&M 172 is completed. This contains the preliminary information, the event number, and the event classification. This documentation is required to be completed within 24 hours**[3] **of the event occurrence**.**]**

[3] The 24-hour time may be extended with appropriate documentation (e.g., email) from the manager responsible for the equipment involved, but no more than the next business day following the event.

12.1 Minor Events

[Minor events are documented on the PO&M 172 by the Restoration Team.] Event data collected by the Restoration Team is either entered into the PO&M 172 or is attached as a PDF. [**The Event Analysis and Findings are also documented on the PO&M 172 Part II within 10 business days following the report of the event. This is forwarded to the manager responsible for the equipment or facility for approval and development of a Corrective Action Plan, as needed.**]

12.2 Significant Events

[Significant Events have preliminary information documented on Part I of the PO&M 172. The information gathered or developed by the Restoration Team is submitted to the Investigation Team. The Investigation Team compiles the Event Data, including data collected by the Restoration Team, restoration analysis, and the restoration actions. The Investigation Team assembles the documentation in the example outline provided in "Appendix D, Incident Investigation Report Outline," or as defined in the Charter. The documentation includes a description of the event and what caused the event. If the evidence indicates contributing factors to the cause of the event, they also will be included in the documentation. These findings are submitted to the Sponsor.] This process may occur through two rounds—a draft and final within the timeframe defined in the commissioning charter. The draft report will ensure that the scope of the investigation is satisfied and that no follow-up investigation is required. Comments on the draft report are to be sent to the Investigation Team. [**All comments must be addressed by the Investigation Team through either a clarification response or modification of the report resulting in a final report submitted to the Sponsor. Any findings that involve compliance with NERC or WECC reliability standard requirements must be reviewed and concurred as described in Section 13**.]

[A Corrective Action Plan is to be developed by the office responsible for managing the equipment or facility and based on the final report.] This event documentation and Corrective Action Plan are submitted to the Regional Director and is available for dissemination within Reclamation.

12.3 Severe Events

As in the case of Significant Events, Severe Events have preliminary information documented on Part I of the PO&M 172. [**The information gathered or developed by the Restoration Team is submitted to the Investigation Team. The Investigation Team compiles the Event Data; including data (restoration analysis and the restoration actions) collected or developed by the Restoration Team. The Investigation Team assembles the documentation**

following the example outline provided in appendix D or as defined in the Charter. The documentation includes a description of the event and what caused the event. If the evidence indicates contributing factors to the cause of the event, they also will be included in the documentation. These findings are submitted to the Sponsor. This process may occur through two rounds—a draft and final within the timeframe defined in the commissioning charter. The final draft should be submitted to the Regional Director for comment by the Sponsor.] The draft report will ensure that the scope of the investigation is satisfied and that no follow-up work is required. Comments on the draft report are sent to the Investigation Team. [**All comments must be addressed by the Team through either a clarification response or modification of the report resulting in a Final report submitted to the Sponsor. Unlike the Significant Event, the final documentation for Severe Events is submitted to the Commissioner's Office by the Sponsor with a courtesy copy to the Regional Director. The documentation submitted to the Commissioner's Office is used by the office responsible for managing the equipment or facility to develop a Corrective Action Plan. The Corrective Action Plan is submitted through the Regional Director to the Commissioner's Office separately from the event documentation**.] Once both are reviewed by the Commissioner's Office, they are available for dissemination.

13. Compliance Review

The regions may perform a compliance review of every completed PO&M 172 to identify any FERC Order 693 NERC or WECC reliability standard requirements that may be applicable and to determine if the requirement was met. [**If a potential compliance violation is suspected, the regional compliance reviewer will coordinate with the PRO Reliability Compliance Manager. The PRO Reliability Compliance Manager, or designee, will conduct a review of every completed PO&M 172 where FERC Order 693 NERC or WECC reliability standard requirements may be applicable and to determine if the requirements were met. The PRO Reliability Compliance Manager will coordinate with SSLE on any PO&M 172s NERC or WECC reliability standard requirements which involve SSLE. The review will be documented on Part IV of the PO&M 172.]**

The regions may perform a compliance review of every completed PO&M 172 to identify any FERC Order 706 NERC or WECC reliability standard requirements that may be applicable and to determine if the requirement was met. [**If a potential compliance violation is suspected, the regional compliance reviewer will coordinate with the CIO Reliability Compliance Manager. The CIO will conduct a review of every completed PO&M 172 where FERC Order 706 NERC or WECC reliability standard requirements may be applicable and to determine if the requirements were met. The CIO will coordinate the results of the review with the PRO Reliability Compliance Manager. The PRO**

Reliability Compliance Manager will document the review on Part IV of the PO&M 172.

Findings in all draft Investigation Reports that involve reliability compliance must be reviewed by the PRO to ensure consistency with Reclamation's interpretation of compliance. The PRO will ensure coordination of the review with either the CIO or SSLE as appropriate.]

The investigation team may discover that a possible compliance violation occurred in its evaluation of the event. To ensure consistency with the interpretation of the NERC or WECC Reliability Standard requirements, the Team lead will ensure that the draft report with findings are reviewed by the PRO Reliability Compliance Manager. In addition, [**if any comments submitted to the Investigation Team contest the findings which are associated with NERC or WECC Reliability Standard requirements, the Investigation Team lead will consult with the PRO Reliability Compliance Manager and Power Resources Office Manager on those findings. The resulting consensus interpretation and disposition of the specific findings which were contested will be included in written communication with the Sponsor within two weeks.]**

14. Corrective Action Plan

[**Corrective Action Plans are developed by the office responsible for managing the equipment or facility.**] The focus of the Corrective Action Plan is to prevent the recurrence of the event and to reduce the number of recurrences. [**The Corrective Action Plan addresses each of the findings contained in the event documentation. The plan contains specific timetables and priorities for each finding in which an action is developed to prevent recurrence. Management of the Corrective Action Plan is the responsibility of the office that developed the plan. Corrective Action Plans must be completed in the timeframe listed**.] Sometimes, there are situations when the only option available, due to lack of event information, is to monitor facility equipment to gather more information.

[**Corrective Action Plans will be tracked to completion. Periodic review of the Corrective Action Plans shall be performed by the office organizationally one level higher than the office responsible for managing the facilities or equipment involved in the event, because this is a good internal control practice to ensure that Corrective Actions are effective, appropriate, and complete**.] In some cases, the office organizationally one level higher will be the Regional Power Office. CARMA should be considered for tracking Corrective Action Plans to completion.

[**When the Event Report and Corrective Action has been developed, each region will post a PDF version of the Event Report and Corrective Action Plans to the Power Resources Office Share Point Web site, upon receipt of the event documentation from either the Restoration or Investigation Team, for Minor Events or Incidents, respectively.]** PDF documentation of Minor Events or Incidents may alternatively be linked to the appropriate folder in the PRO Share Point for access by the PRO staff, if that region chooses to maintain its own Share Point website. **[The regions will review Event Reports and Correction Plans to ascertain if similar events are occurring within the region and disseminate the findings among the offices of the region. The PRO Incident Evaluation Program Manager will review all event documentation from either the Restoration or Investigation Team, for Minor Events or Incidents, respectively once it is posted on the PRO Share Point or made available to the PRO Share Point within 15 business days. Events which are similar, involve similar equipment problems among regions, or who's Finding or Corrective Action Plans could benefit a region will be disseminated to that region.]** The review will be tracked through a logging system to provide a continuous status of which events have been reviewed and the date of the review. The logging system will be posted on the same PRO Share Point Website used for all event documentation. **[The PRO Incident Evaluation Program Manager will consolidate and evaluate Event Reports and Corrective Action Plans for similar events and disseminate the findings among the regions.**]

Corrective actions may include actions handled in accordance with appropriate human resource office procedures. [**While tracking these actions to completion is paramount to preventing recurrence, the information associated with the specific action is redacted to protect the privacy of all involved prior to any dissemination of the Corrective Action Plan**.]

14.1 Minor Events

[**Corrective Action Plans for minor events are developed within 5 business days following receipt of the PO&M 172 from the Restoration Team. The manager responsible for the equipment or facility involved in the event is responsible to ensure that the findings identified by the Restoration Team are addressed in the Corrective Action plan, which is added to Part III of PO&M 172. This is indicated by the manager's signature**.]

14.2 Significant Events

[**Significant Events are more complicated, and more time is allotted for developing the Corrective Action Plan. The Corrective Action Plan for Significant Events is completed within 10 business days following receipt of the final investigation documentation from the Sponsor**.] The Corrective

Action Plan is appended to the event documentation and submitted to the Regional Director's Office.

14.3 Severe Events

[Severe Events have more time allotted for developing the final Corrective Action Plan than what is allotted for Significant Events. The Corrective Action Plan for Severe Events is to be completed within 20 business days following receipt of the final investigation documentation. The Corrective Action Plan is submitted to the Commissioner's Office for review and concurrence.]

15. Unexpected Event Reporting Program Evaluation

The Unexpected Event Reporting program success will be accomplished if all events are documented and reported, there are no recurring events, and there are no similar events in two regions. A program success also depends on the value it provides to those who use the information. [**The PRO will carry the primary responsibility in evaluating the success of the program and recommending changes through evaluating the program every 2 years.**]

15.1 Unexpected Event Reporting Improvement

The Unexpected Event Reporting Program strives for improvement in achieving its stated purpose. This requires the active involvement of all participants in the program to recognize and comment on meaningful avenues for improvement. All aspects of the program are open for comment, including the following:

1) Modification of governing Directives and Standards.
2) Improvements in this FIST volume.
3) Event evaluation, reporting, and Corrective Action Plan processes.
4) Post event tracking.
5) Training on Unexpected Event Reporting.
6) Recommendations for improving the Unexpected Event Reporting Program should be directed to the Manager, Power Resources Office, 86-61600.

15.2 Measurement of Compliance with FIST

This is the measure if the procedures described in this FIST[4] are being followed. This can be measured for power facilities by comparing the reported forced outages that are reported through the O&M 59 system or the reported event in the station log to the events recorded through this program. This also would include the information gathered by the regions relating to the Corrective Action Plans. For SCADA equipment, the measurement would be by comparing the Reclamation Enterprise Service Center (RESC) event logs for the specific systems to the events recorded through this program. The measure also is to be based on the number of events of a similar nature or with similar equipment in more than one region.

15.3 Analysis of Compliance with FIST

[**The data will be examined to ascertain if the number of reoccurring events is reduced. The data will be used to analyze the quality and the appropriateness of the Corrective Action Plans as determined by the regions. This analysis will be performed by the PRO.**] The analysis would use an appropriate statistical evaluation of the event types. The analysis needs to examine if similar events are found or events involving similar equipment problems are found to have occurred in more than one region.

15.4 Program Value

The benefit of the program would be measured primarily through the use of surveys. Surveys would be conducted to ascertain if the information provided through reporting and investigations has provided a benefit to the operating offices. [**A periodic survey of regional, area, and operating offices will be conducted by the PRO to determine if the quality of information from investigations and data collected in event reporting has contributed to reducing events. The survey will also solicit feedback for improvement**.]

15.5 Program Adjustments

[**The information collected and analyzed will be used to develop changes to this FIST. These changes will be developed by the PRO in coordination with the regions and presented to the Power Managers for consideration.**]

[4] The measure would include a variance if they are different than the procedures in this FIST.

Appendix A
Power O&M 172

POWER O&M UNEXPECTED EVENT REPORT

Region:	Project:	Report Number:

Name of Facility:	Date of Event:	Time of Event:	Duration of Event:

NERC Function (Check applicable function):		Generator Data (Three letter facility designation followed by Unit numbers and actual MW that tripped offline with this event):	Transmission (Facilities that tripped off –line with this event):
TO	☐		
GO	☐	(ex. HOVA1)	
GOP	☐	MW	

PART I
PRELIMINARY REPORT OF ALL UNEXPECTED EVENTS

1) **DESCRIPTION OF EVENT OR CONDITION** (For the event or condition, who was involved, what equipment or system(s) were involved and where did it occur, what work or activity was being done, what was the result, what or how did the event start or how was it found, and any other information you believe needs to be included. Use additional space or pages as needed. Also include basis for why the possible sabotage is suspected.)

2) **INITIAL REPORT OF EVENT BY**:

a) NAME(s)	b) DATE OF REPORT

3) **POSSIBLE SABOTAGE SUSPECTED** ☐ Yes ☐ No
SSLE to review suspected sabotage determination and take appropriate action

4) **CLASSIFICATION** ☐ Minor ☐ Significant ☐ Severe
If this Event is classified Minor, complete the PARTs II and III.
If the Event is classified as Significant or Severe PARTs II and III information will be included in a separate Investigation Report and Corrective Action Plan.

5) **ACTIONS TAKEN** (Include any actions taken to restore equipment to service. Use additional space or pages as needed.)

6) **RESTORATION TEAM**

PART II
MINOR EVENT - REPORT

1) EVENT DATA (Use additional space or pages as needed. Include a sequence of event data and other data, or attach PDF files)

2) EVENT ANALYSIS (Use additional space or pages as needed.)

3) RELAY AND PROTECTION SYSTEM OPERATION OCCURRED AS PART OF UNEXPECTED EVENT OR CONDITION

Did the Protection System (relays, CTs, PTs, DC systems, batteries, etc), operate as expected? ☐ YES ☐ NO

If the answer is NO, then in the following sections **specifically** address, for each component that did not operate or function as expected:

1) the cause(s) of the misoperation;
2) any conclusions that can be drawn from event;

4) **FINDINGS (**Use additional space or pages as needed.)

Use the space below to provide the specific information. (Use additional space or pages as needed.)

PART III
MINOR EVENT - CORRECTIVE ACTION PLAN

1) **CORRECTIVE ACTIONS (**Indicate here if further investigation is necessary. Use additional space or pages as needed. Each finding related to a Protection System misoperation will need to have its own Corrective Action Plan. Accomplishment of the Corrective Action Plan will need to be tracked and documented.)

2) **COMPLETION DATES FOR ACTIONS LISTED IN Part III 1)** (This is a suggested date not the actual accomplishment. Use additional space or pages as needed.)

3) **CORRECTIVE ACTION PLAN APPROVAL BY**:

a) **NAME**(s) **AND SIGNATURE**(s)	b) **DATE OF REVIEW**

4) **DISTRIBUTION OF REPORT**

A copy of this report, should be sent to the Area Manager, Regional Power Manager, Facility Manager, Safety Manager, and Restoration Team members.

PART IV MINOR EVENT - COMPLIANCE REVIEW			
Part III Findings	Corresponding Part III Corrective Action	Applicable Standard and requirement number	Compliance Violation (Yes/No)
Individual Performing Compliance Review:		Date:	

Appendix B
Example of an Investigation Team Charter

RECLAMATION
Managing Water in the West

Incident Investigation Team Charter

Version 1.0

U.S. Department of the Interior
Bureau of Reclamation
Denver, Colorado

November 2010

Charter Approval

The Sponsor (manager or designated representative of the office organizationally one level higher than the manager of the office organizationally responsible for the equipment or facility involved in the event) authorizes the attached Charter:

Sponsor

Name Title/Role/Office	Signature	Date
Name Title Sponsor Office		

This Charter is effective as of the date of approval by the Sponsor and signed by the respective Team Members. The Charter sections may be revised as necessary by the Sponsor. The Charter will reflect the date of the most recent approved revision and distributed to all Team Members.

Investigation Team Members

The following Investigation Team Members are in agreement and support the attached Charter and commit to fulfilling their roles and responsibilities to the best of their ability.

Member	Signature	Date
Team Member Name/ Team Lead/ Power Operations Office		
Team Member Name/ Team Member/ Power Resources Office		
Team Member Name/ Team Member/ Infrastructure Services Division		
Team Member Name/ Team Member/ Hydroelectric Research		
Team Member Name/ Team Member/ Central Valley Operations Office		

Revision History

Version	Date	Modified Sections	Summary of Changes
1.0	11/11/09		

Purpose

The purpose of this Charter is to establish the Incident Investigation Team for the purpose of Investigation the Incident number YYYYMMDDFAC#.

Business Need

Since the consequences of these incidents can be very costly either in terms of equipment damage, lost revenue, or jeopardy to life and property, it is necessary to place emphasis on a program to eliminate or reduce all Incidents. To promote improvement in operations and maintenance procedures, each Incident must be reviewed and reports prepared. To profit from such experiences, it is necessary to analyze existing problems and study recommended solutions. Written reports are intended for this purpose.

By fully investigating the Incident and determining the cause, the recurrence of the Incident may be prevented in the future. The Incident has been determined to have had a significant impact and warrants through data gathering and evaluation. The use of a team of subject matter experts will ensure a complete investigation and full consideration of the facts, as well as determination of the cause, to the degree that it can be determined.

Background

Reclamation historically has conducted a formal program of evaluation and reporting of incidents affecting Power Operation and Maintenance (O&M). Reporting of major incidents was required under Reclamation Instructions, Part 252.3.3, which were “sunset” in the early 1990s. Various reporting requirements were originally established in Power O&M Bulletins and later in Facilities Instructions, Standards, and Techniques (FIST) volumes.

In May 1996, following several incidents of concern in the power program, the Commissioner established a “Power O&M Team” to review the power program for effectiveness and make recommendations to address any problems found. One recommendation from this team was to “reinvent” the Power Operation and Maintenance Incident Evaluation and Reporting (Power Incident Evaluation) providing more authority and structure.

Scope

The Investigation Team (Team) is commissioned to evaluate the data actions taken immediately preceding the event. If the event analysis indicates that a Cyber Asset (a programmable electronic device or communication network

device) contributed to the event, the RESC needs to be notified to invoke Reclamation's Information Technology Incident Response Procedure. The Team is expected to assemble and develop an outline of the investigation similar to the one provided in FIST 6-3. The Team will have access to all operations and maintenance data related to the event. The staff of the office responsible for managing and operating the equipment or facility will be made available to the Investigation Team for interviews. The Team will conduct onsite evaluations as indicated in the following sections of this Charter. The Team is required to submit a draft report as indicated in the following sections of this Charter. The draft will include all data used for analysis as well as all interview notes. The draft report will follow the outline established in the following sections of this Charter. The Team may receive comments on the draft report and will address those comments in the final report. A final report will be submitted to the Sponsor as indicated in the following sections of this Charter.

Testing Data

To the degree required, the Investigation Team may request that a specific test be conducted of equipment or facility operations. These tests need to be coordinated in advance. Data from tests performed prior to the event will be provided within 1 week following the request.

Expenses

The Investigation Team is authorized to use the following cost authorities as described in the table.

Expense	Cost Authority	Cost Authority	Split	Remarks
Travel	U4P155700010010101	A40155700010010101	20/80	Please split the costs concurrently as indicated
Per diem				
Labor				
Printing/ miscellaneous				

Communication

The Investigation Team lead is represented by the Investigation Team Leader listed in the Charter. Requests from the Team will be presented by the Team lead to the Manager of the office responsible for the equipment or facility.

Communication with the Team by the office responsible for the equipment or facility will be directed to the Team Leader. The Team Leader will contact the Manager of the office responsible for the equipment or facility within 2 days following the execution of this Charter. The Team Leader is responsible to communicate Investigation status and Investigation Team issues with the Charter Sponsor.

Roles and Responsibilities

The following chart summarizes the role and responsibilities of the individuals involved in this Charter.

Roles	Responsibilities
Sponsor	• Authorize funds for the Investigation. • Commission the Investigation Team. • Primary contact point for Investigation Team Leader in investigation issues. • Ensure Investigation Team is free from undue influence. • Enforce the Charter. • Receive the draft Investigation Team report and forward the report to the responsible manager(s) of the equipment or facility involved in event. • Coordinate comments on draft report with Team Leader. • Receive and distribute Final Investigation Report.
Team Leader	• Provide leadership for Investigation. • Coordinate Investigation logistics. • Communicate status and issues with the Sponsor. • Enforce the Charter requirements. • Ensure that the draft report is consistent with FIST or local practice regarding Incident investigations. • Ensure completion of the Investigation. • Ensure the Investigation draft report is submitted to the Sponsor. • Address comments received on draft report. • Finalize the Investigation Report.
Team Member	• Conduct Investigation consistent with the FIST or local practices regarding Incident Investigations. • Meet the requirements of this Charter. • Follow the guidance of the Team Leader. • Submit information and products as required by the Team Leader.

Deliverables

The Investigation Team will develop an outline of Investigation within _____days of execution of this Charter and submit the outline to the Sponsor.

The Team is expected to assemble within _____ days of the execution of this Charter.

The Team will conduct on site evaluations within _____week(s) after execution of this Charter.

The Team will complete the Investigation within _____ weeks.

The Team will deliver a draft report to the Sponsor by _____.

The Team will address all comments received within _____ weeks of receiving the comments.

The Final Investigation report will be submitted to the Sponsor within _____ week(s) of receiving comments.

The Investigative Team understands that if, at any point during the operational investigation process, sabotage or criminal activity is suspected to be a causal factor, work will be suspended and local sabotage and emergency notification procedures will be followed. Criminal investigations, including the preservation of criminal evidence, must be conducted by qualified law enforcement officials and will take precedence over any actions by the Investigative Team.

Appendix C
Specific Tasks and Timelines Associated with Unexpected Event Reporting

Specific Tasks and Timelines associated with Unexpected Event Reporting

The figures 1 and 2 depict the event documentation process. The following is the general time lines and responsibilities associated with the documentation. The time table associated with the Incident reporting will be defined in the Charter.

Task	Timeframe	Responsibility
Enter the Preliminary Event information in the PO&M 172.	Immediately after receipt of information but within 24 hours.	Operations Office.
Get a Restoration Team to the site.	Immediately after receipt of information but within 24 hours.	Operations Office/Maintenance Office.
Select the appropriate Event Classification on the PO&M 172.	Immediately after receipt of information but within 24 hours.	Operations Office/Maintenance Office.
Indicate if the event is possible sabotage and enter the information on the PO&M 172. If possible sabotage, report it.	Immediately after receipt of information but within 24 hours.	Operations Office/Maintenance Office.
Complete Part I of the PO&M 172.	Within 24 hours of the initial report of a Minor Event.	Operations Office.
Complete Part II of the PO&M 172.	Once restoration is complete, within 10 business days of the initial report of a Minor Event.	Restoration Team.
Investigation Team assignment through Charter.	Within 5 business days of a Significant Event. Within 5 business days of a Severe Event.	Sponsor.
Incident Investigation outline.	As determined in the Charter.	Investigation Team.
Incident Investigation outline.	As determined in the Charter.	Investigation Team.
Incident onsite evaluation.	As determined in the Charter.	Investigation Team.
Incident Investigation completion.	As determined in the Charter.	Investigation Team.
Draft Investigation Report.	As determined in the Charter.	Investigation Team.

Task	Timeframe	Responsibility
Final Investigation Report	As determined in the Charter.	Investigation Team.
Corrective Action Plan.	Within 5 business days following receipt of PO&M 172 for Minor Events. Within 10 business days following receipt of Final Report for Significant Events. Within 20 business days following receipt of Final Report for Severe Events.	Manager responsible for the equipment of facility involved in the event.
Event Documentation Review	Within 15 business days of posting	PRO Incident Evaluation Program Manager
Compliance Review	Within 15 Business days of posting	PRO/CIO Reliability Compliance Manager

Appendix D
Incident Report Outline

I. Date of the Incident.

II. Location of the Incident.

III. Description of the Incident

IV. Conditions prior to the Incident

V. Sequence of events.

VI. Analysis of the Incident.

VII. Supporting facts.

   a. Statements.

   b. Reports, including reports or tests conducted in conjunction with the investigation or prior to the incident and used to verify the condition of the equipment involved in the incident.

   c. Calculations supporting analysis.

VIII. Conclusion from the analysis (in the order of the timeline).

IX. Findings.

X. Issues to be considered that may have contribution to the event.

Appendix E
Investigation Processes

Investigation Process

I. PURPOSE

The Incident investigation is conducted to determine the apparent cause(s) of an Incident to document and record, and prevent a similar occurrence. Generally, an Investigation Team of one to five members is appointed for this purpose. The Incident Investigation Team has several major functions:

(1) Conducting a comprehensive investigation within the defined scope, collecting all pertinent information, and determining the facts relevant to the incident.

(2) Analyzing the facts and determining causal factors that contributed to the incident, with particular emphasis on determining the root causes.

(3) Identifying issues that should be addressed to prevent recurrence of the incident.

(4) Reporting the essential facts, findings, and results of the investigation clearly and concisely.

(5) Maintaining appropriate communications with interested organizations throughout the investigation.

(6) Ensuring the quality, accuracy, and safety of all its activities.

To meet the above criteria, an Investigation Team should be comprised of members who collectively have adequate technical expertise pertaining to the type of incident and facility where it occurred, have suitable investigation experience, and have organizational and reporting/writing skills. In addition, training in root cause analysis technique may be helpful in analyzing complex failures. Depending on the nature of the event, a one-person Investigation Team may be sufficient. However, for most Incidents, generally two or more persons are necessary to provide the required collective expertise.

II. INVESTIGATION PROCESS

Once Investigation Team members have been appointed, the following general tasks are recommended for the Investigation Team process, keeping in mind that the Incident complexity determines which tasks are more applicable.

(1) **PRIOR TO ARRIVAL ONSITE**

(a) Study the facility organization chart and identify key facility personnel who can assist the Investigation Team (e.g., safety, industrial hygiene, plant operations, etc.). Schedule any clearances needed.

(b) Review facility documentation showing major features, such as power equipment electrical single-line diagrams and mechanical, hydraulic, or structural drawings as appropriate. Valuable time can be lost at the scene if the team is not familiar with the basic type and operation of pertinent equipment and/or structures involved in the incident. The Investigation Team technical expert(s) should take the lead.

(c) Instruct appropriate facility personnel to preserve physical evidence and minimize unnecessary post incident disturbance to the site. It is difficult to predict how any evidence can impact the course of an investigation; therefore, the incident site should be altered (stabilized) only as necessary in consideration of the immediate safety and operation of the facility. Any material that has to be removed from its original location prior to arrival of the Investigation Team should be cataloged, minimally disturbed, and suitably stored for further inspection.

(d) Request eyewitnesses and other key personnel (coworkers, supervisors, managers, injured parties, incident scene responders, fire department and medical personnel, etc.) prepare written descriptions of what they saw and how they responded to the incident. Make arrangements to interview these people when onsite.

(e) Arrange for a dedicated Investigation Team room at the facility to provide isolation and privacy for the team to conduct employee interviews and to maintain confidentiality of investigation materials.

(f) Work with local staff to acquire a site Job Hazard Analysis (JHA) and equipment clearance as necessary. Details of the JHA and clearance can be worked out once the Investigation Team arrives on site.

(g) Determine what personal protective equipment, training/testing (e.g., respirator usage), and medical clearance are required onsite. In some instances, hazardous materials or byproducts can be present at the scene. The facility safety manager should assist the Investigation Team in determining appropriate protective action. Failure to anticipate hazards and prepare for them ahead of time

can delay the team upon arrival and possibly expose them to hazardous substances onsite.

(2) **CONDUCTING THE INVESTIGATION**

Incident investigation should be a methodic process from gathering evidence through determining facts and causal factors to reporting findings and recommendations. Initially, an Investigation Team might feel as if the incident scene and investigation are in a state of controlled chaos. This is natural; but as the investigation process takes hold, a sense of order should prevail, and the facts and causal factors should become apparent. Incidents generally have several contributing causal factors and inappropriate actions. These factors and actions can be attributed to a variety of issues including, but not limited to, improper facility operation and maintenance (O&M) processes, employee behavior, safety culture, or management processes and controls. The investigation should accurately identify all of the significant issues. Often times, the conditions allowing an incident to occur develop over time, requiring the Investigation Team to review historical records. Resources and investigation tools to help the team accomplish their task are listed below.

(a) This FIST volume

(b) Copy of recent incident investigation reports

(c) Copy of facility policy, procedures, and other pertinent documents provided by the site personnel

(d) U.S. Department of the Interior video tape: *Just-in-Time Serious Accident Investigation Training*, April 2, 1998 (19:12)

(e) Gathering and preserving evidence

(f) Testing physical evidence

(g) Conducting interviews

(h) Determining facts

(i) Events and causal factors charting

(j) Previously issued, related CARMA trouble reports, and work orders

If at any time during the operational investigation process, the team suspects sabotage or criminal activity, work must be suspended, and local sabotage and emergency notification procedures must be followed. Criminal investigations, including preservation of criminal evidence, will be conducted by a law enforcement officer and take precedence over any actions by the operational investigative team. Law enforcement officials will factor facility and personnel security

and safety into their investigation process and may rely on input from the investigative team or other local staff to support security and safety efforts.

(3) **ROOT CAUSE ANALYSIS**

A root cause analysis should be conducted for most Incidents. The methodology used is not as important as the results. In Incident Investigation, it is important to look beyond the errors and failures that immediately precipitated the incident. The Investigation Team should identify if there are any system deficiencies at the work and management levels to determine the underlying oversights, omissions, performance errors, and accepted risks that can be specifically identified as the root causes to the Incident. These causes may lie in the organizational structure, safety management systems, or line management processes related to the Incident.

(4) **GATHERING AND PRESERVING EVIDENCE**

As soon as possible, the Investigation Team should inspect the scene for familiarity, make initial notes and documentation, and control the evidence. Records should be made of pertinent information such as original location, orientation, relative size, condition, etc., of items involved in the incident. The entire scene should be well photographed. Sketches and videotaping also can be useful. As the investigation progresses, detailed photographs should be taken to record key evidence, support findings, and document the investigation process, including disturbance to the scene. They should be carefully identified and logged to show the date, time, and purpose of each photograph. Keep in mind that photographs may be the only means to re-examine critical evidence after the original condition of the scene is disturbed.

Physical evidence can be fragile. Objects can be removed, broken, lost, or misplaced, cleaned, destroyed, or distorted. When physical evidence is identified, it is collected and secured or the area in which it is located is secured to preserve integrity of the evidence. Materials can be bottled, bagged, or boxed and their locations recorded (photographed). The Incident scene should be barricaded (roped or taped), doors locked, guarded, or preserved by other means.

(5) **TESTING PHYSICAL EVIDENCE**

Testing and analyzing physical evidence may be important tools in identifying apparent causes. Testing may be nondestructive or destructive in nature and, therefore, should be properly sequenced in the investigation process. Testing may be witnessed or performed by members of the Investigation Team onsite or performed by an independent laboratory off site as necessary. Certain testing of

equipment (e.g., electrical controls) may involve intermittent problems that are potential causes requiring careful assessment to accurately diagnose. Keep in mind that some equipment may not respond to post-event testing in exactly the same way it might have before the incident, due to collateral stress or damage. The Investigation Team should well understand the equipment or materials to be tested, test procedure, and possible outcomes and should request appropriate expertise from facility personnel to assist in conducting tests on site. Possible positive test indicators can be:

(a) Total equipment failure

(b) Abnormally slow, sluggish, or partial operation

(c) Overload or out–of-range operation

(d) Intermittent or incomplete operation

(e) Out of calibration or tolerance limits

(f) Excessive noise, vibration, or heat

(g) Improper position or status indication

(6) **CONDUCTING INTERVIEWS**

After the Investigation Team arrives on scene, a witness interviewing schedule should be established, and interviewing should begin as soon as practical. Eyewitnesses can forget, overlook, or fail to recall critical evidence. Individuals naturally begin to rationalize the circumstances of traumatic accidents after the event. Therefore, interviewing should be conducted before the witnesses or participants leave the scene, when possible. A neutral and private location free from distractions (Investigation Team room) should be reserved for these interviews. Each team member is responsible for ensuring that the interviews are productive. Good interviewing techniques that aid in this effort include the following:

(a) Plan the interview. Determine ahead of time what information is needed and what questions need to be asked.

(b) Establish rapport before the interview starts. Create a comfortable environment for the witness. Do not treat the interview like an interrogation. Explain the purpose of the investigation (facts finding, root causes) and that it is not to place blame or levy punishment.

(c) Provide a standard opening statement to ensure consistency for all interviews. Ask the same basic questions of each interviewee and then expand as necessary.

(d) Before questioning the interviewee, ask them to provide a description of the incident in their own words. Do not interrupt during this description.

(e) Include open-ended questions (i.e., questions that cannot be answered by "yes" or "no" responses). Remember that incidents can be traumatic to staff. Be inquisitive but not overbearing.

(f) Be unbiased and nonjudgmental. Do not ask leading questions or suggest a point of view; the witness may believe that a decision has already been made, and any contrary information they provide may not be taken seriously.

(g) Be attentive and take notes during the interview or audio record it with the interviewee's permission.

(h) Schedule time between interviews to reflect on the information obtained and to decide whether any new information has affected the questions planned for the next interview.

(7) **DETERMINING FACTS AND EVENT AND CAUSAL FACTOR CHARTING**

The first step in an Incident Investigation is to determine the facts or what happened. Identifying all the relevant facts through the Investigative process enables the team to satisfy this requirement. As facts are gathered and reviewed, first impressions should not guide the investigation; rather, the Investigation Team should review all facts in the totality of the circumstances to ensure that only factual information is considered for relevance and accuracy; then, validated. Not all information can be established as factual with complete certainty. In some cases, this can be acceptable; however, the team should identify areas of uncertainty in their report and explain why the information is useful and necessary. Keep in mind the following processes when fact finding:

(a) Establish a clear chronological description of the incident (what happened and how). Events and causal factors charting is a powerful tool that can guide the team in establishing all significant facts of the incident. The chart also should help the Investigation Team decide when the investigation is complete (all significant causes have been identified). An example events and causal factors chart is shown in appendix B.

(b) Stress aspects of the incident that could have a bearing on causal factors (e.g., employee training and qualifications, maintenance practices, operational procedure, budget, management controls).

(c) Establish accurate, complete, and substantive information that can be used to support the analysis and conclusions (report) of the Investigation Team discussions. Conduct interviews with additional personnel or have second interviews with previously interviewed personnel as necessary.

III. INCIDENT REPORT AND DEVELOPING FINDINGS

The purpose of an Incident Report is to clearly and concisely convey the results of the investigation in a manner that helps the reader understand what happened, why it happened, and what can be done to prevent a recurrence or improve the Reclamation power program. Investigation results should be reported without attributing individual fault or proposing punitive measures. The Incident Report constitutes an accurate, objective, and factual based document of the team's Investigation process, findings, analysis, and causes of the Incident, conclusions, and findings. The report also should indicate any conditions that might apply to other facilities with similar equipment or processes that could be vulnerable to an event.

Appendix F
Events and How They Are To Be Classified

FIST 6-3 Events and how they are to be classified:

To be covered by FAC 04-02				May be covered by Safety under SAF 01-02	
Nature of impact→ **↓Classification**	**Unexpected Equipment Operation**	**Unscheduled Water Change**	**Loss of Generation**	**Station Equipment Damage**	**Property Damage**
Unclassified within FIST 6-3	Equipment being Commissioned or Tested	Weather Related Events	_____	_____	_____
Minor	All unexpected operations without any other impact	No change to release schedule.	A single protection system operation.	One component damaged	_____
Significant	_____	Unscheduled Change in release schedule with no potential environmental impacts.	More than one generating unit affected by the event multiple protection system operations, or causing more than one event.	A complete station system damaged.	_____
Severe	_____	Uncontrolled release or significant drop in releases either with potential environmental impacts.	More than one powerplant tripped off due to other than one protection system event.	Multiple stations systems or facilities damaged.	Non agency property damaged.

Shaded Cells are defined as Incidents

Appendix G
Suspected Sabotage Reporting Procedures

Purpose

The purpose of these sabotage reporting procedures is to establish and refine procedures to be followed when an unexpected event is suspected to be sabotage that potentially could result in an adverse impact on Reclamation's electric power-related mission capabilities or facilities.

These sabotage reporting procedures are not intended to replace or amend other event or incident reporting instructions or requirements for which individuals or operational components may be responsible. They are intended to address reporting obligations where sabotage is either evident or suspected.

Scope

This guideline applies to all Reclamation-operated facilities, features, and systems; and, in the absence of other response and reporting requirements, these guidelines should be followed by all Reclamation personnel, contractors, and other entities involved in the operation and maintenance of Reclamation electric power-related infrastructure.

Roles and Responsibilities

The majority of the critical roles associated with sabotage response and reporting are defined below. These duties may be identified as ancillary duties for individuals.

- **Witness** – The employee, contractor, or other individual who initially witnesses or identifies a suspected sabotage event or concern.

- **Reclamation Duty Officer (RDO)** – The designated Reclamation employee who has been trained to receive, process, and report incidents according to established procedures and is available on a 24/7 basis.

- **Regional 24-Hour Duty Officer/Regional Emergency Official (REO)** – A rotating, collateral duty position located in each region that is responsible for reporting incidents to the Reclamation Duty Officer.

- **Reclamation Enterprise Service Center (RESC)** – The RESC is Reclamation's Help Desk supporting Information Technology needs, including cyber-related events and incidents.

- **Reclamation Computer Security Incident Response Team (RCSIRT)** – The RCSIRT is a consortium of Information Technology specialists and managers convened, as needed, to address the control of,

response to, and recovery from, incidents and other severe cyber events (including sabotage and potential sabotage events).

Background

Sabotage, as it relates to facilities and systems supporting the Bulk Electric System (BES), is generally considered to be an act by one or more person's intent on disrupting the operations or capabilities of the facilities, systems, or BES. With the exception of intentional acts witnessed and reported directly to local law enforcement, a sabotage event may only become apparent after the analysis of information from various sources. The initial determination that an event is suspected of being sabotage requires locally based operational and situational knowledge, technical evaluation, and information gathering.

Determination of Suspected Sabotage

The initial determination of suspected sabotage occurs in three distinct times during the event documentation process. When looking at the Unexpected Event Documentation Process in figure G-1, these times flow into the off page connector "B" at the bottom of the figure and in figure G-2.

The first time the determination that an event may be suspected sabotage is made is when personnel respond to the event. Personnel who were called to investigate an event should be aware of the indicators listed in attachment A. During the restoration, the personnel who respond to the event may determine that the event was caused by what appears to match the indicators in attachment A. When the determination is made, the personnel charged with restoration will report the determination through the Regional Emergency Notification System. Personnel may be alerted by a witness concerning potential issues associated with the event. The information provided by the witness should be included in the documentation and evaluated accordingly.

The second time the determination may be made is during the event analysis of an event. The analysis should be conducted with knowledge of the indicators listed in attachment A. If the Restoration Team concludes, during the analysis, that the event is suspected sabotage, the Restoration Team reports the determination through the Regional Emergency Notification System.

The third time the determination may be made is when the Power Resources Office (PRO) evaluates Part I of PO&M 172. The PRO may determine that the events have a similarity to other events which warrant further investigation as possible sabotage. The PRO will alert the Security, Safety, and Law Enforcement (SSLE) of the determination immediately.

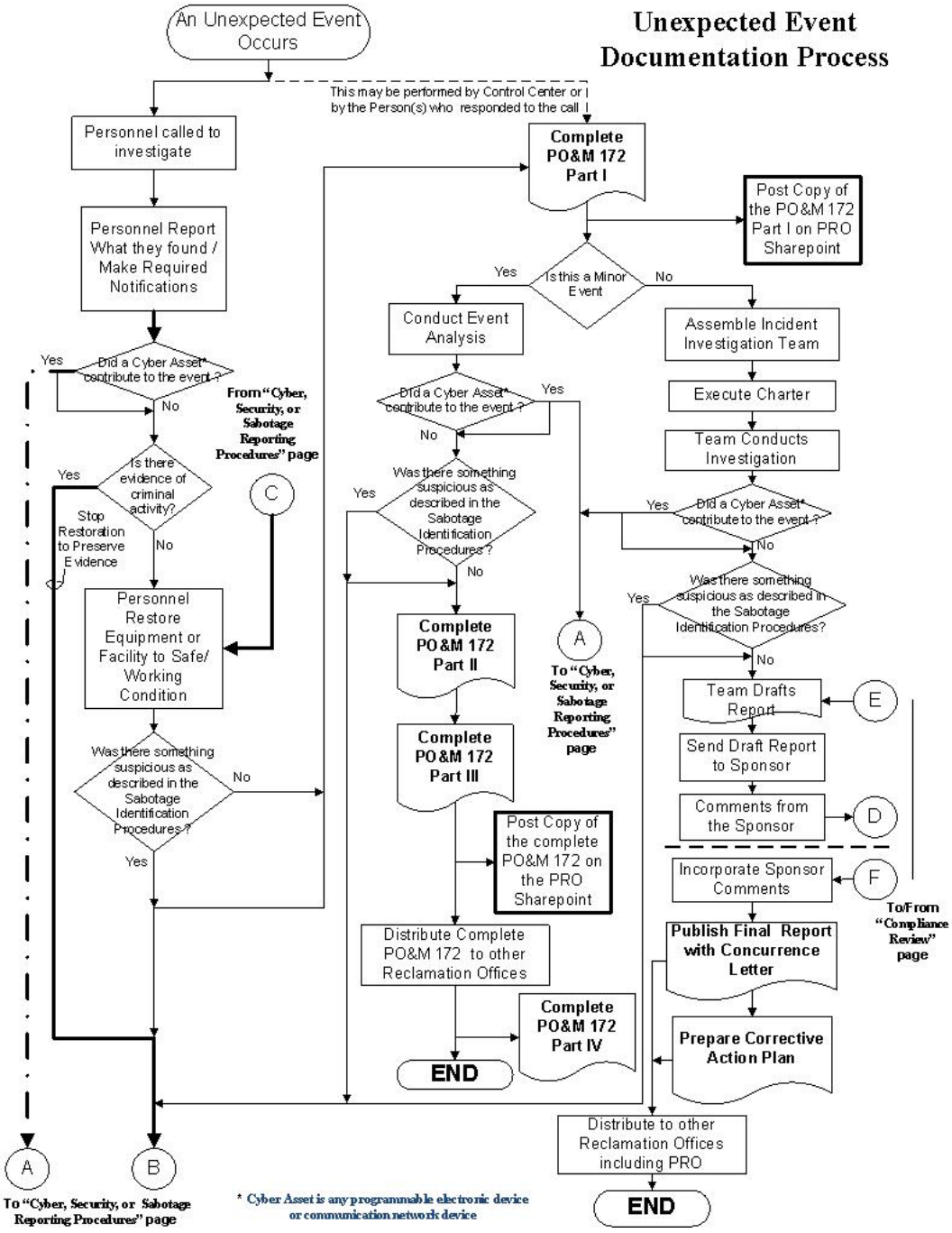

Figure G-1. Unexpected Event Documentation Process.

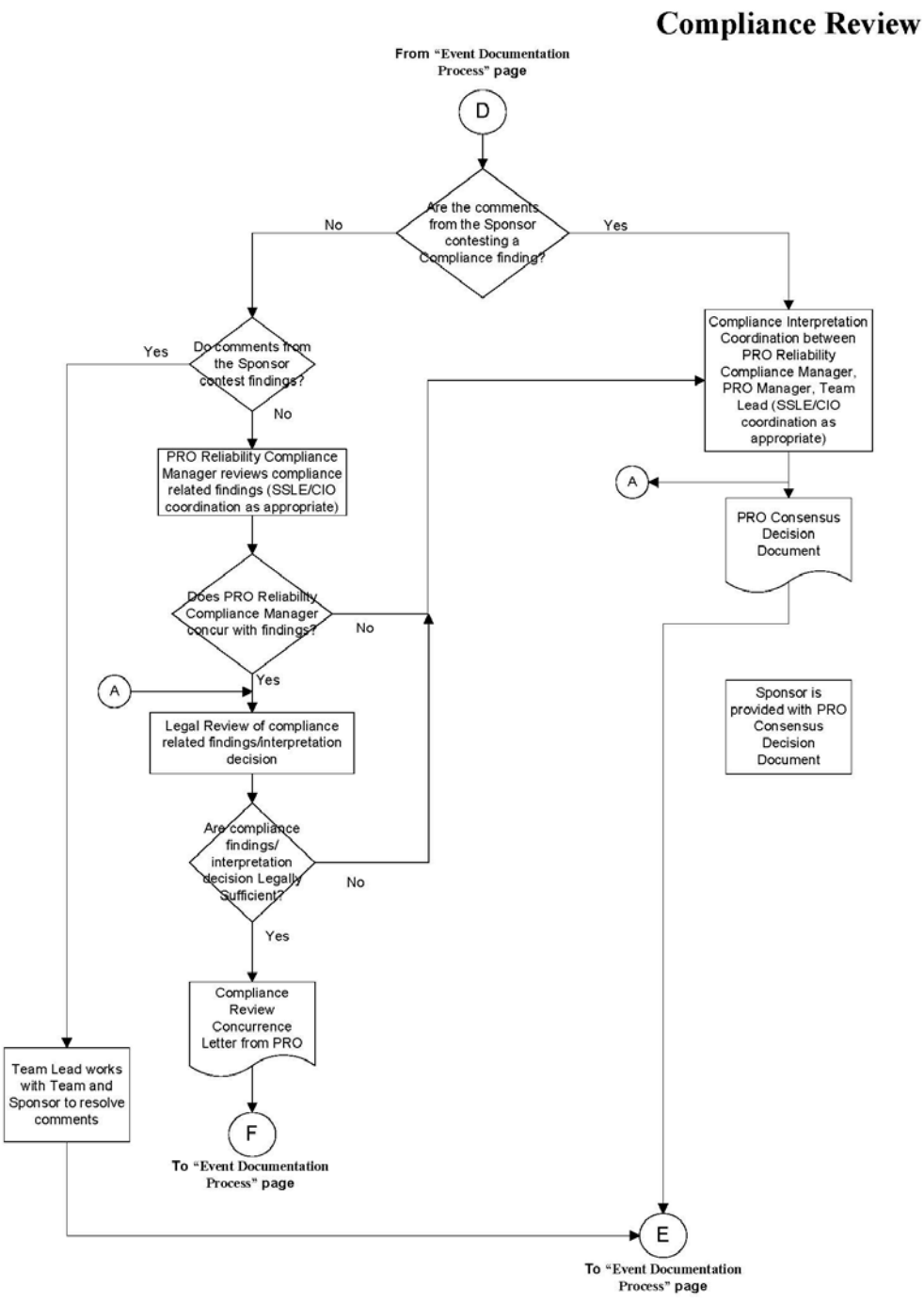

Figure G-2. Compliance Review.

CYBER, SECURITY, or SABOTAGE REPORTING PROCEDURES

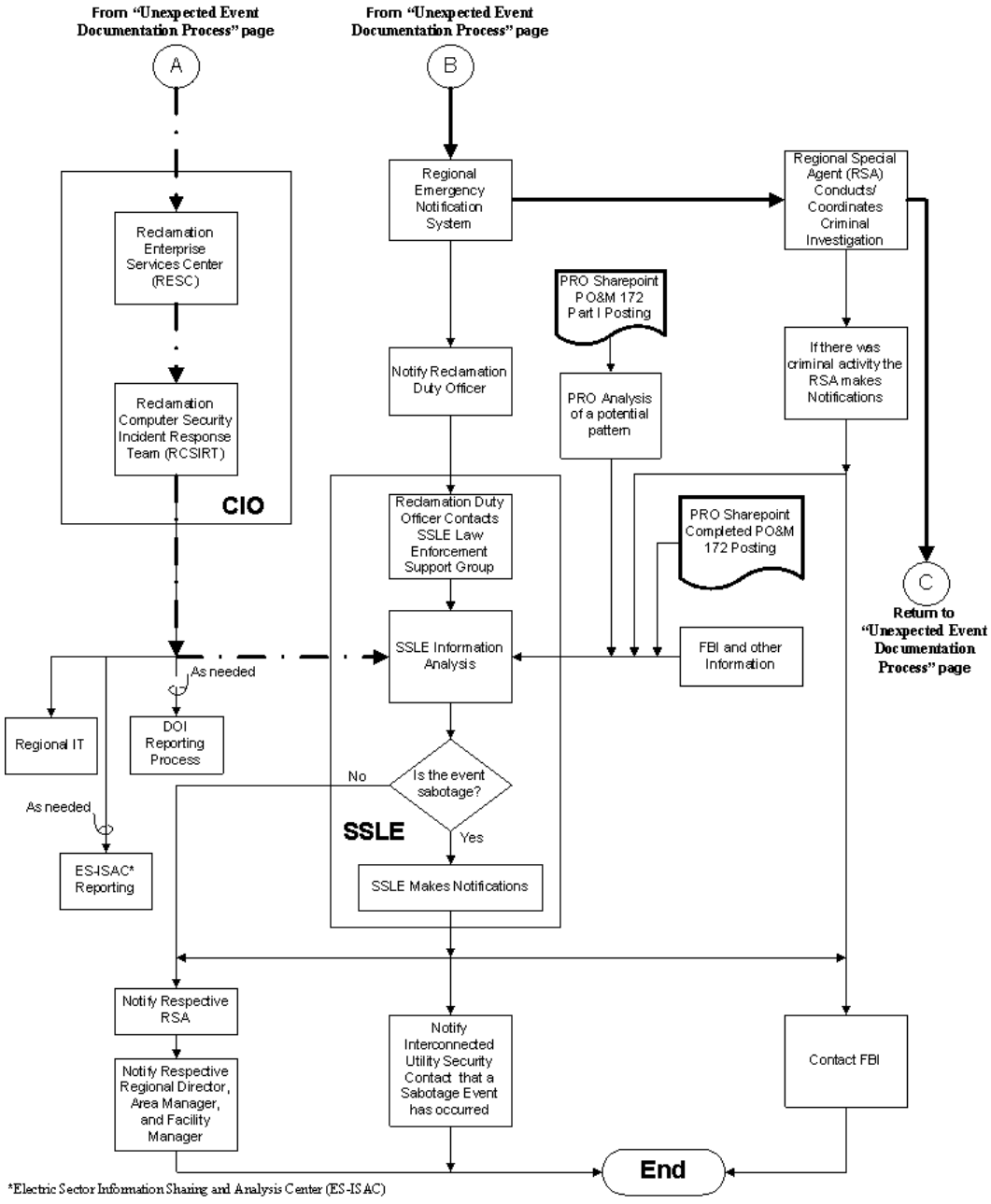

Figure G-3. Cyber, Security, and Sabotage Reporting Procedures.

Reporting of Suspected Sabotage

A general list of suspected sabotage precursors and indicators can be found in attachment A. While this list is fairly inclusive, it does not cover every potential "what if" scenario. [**If something unexplained happens that either does or has the potential to disrupt Reclamation's power operations and the event is considered potentially indicative of sabotage, it should be reported in accordance with these sabotage reporting requirements and guidelines.]**

Notwithstanding other reporting requirements, [**all suspected sabotage events or activities should be reported in accordance with the instructions outlined in this guidance. Events where no reasonable explanation exists for an unusual or disruptive occurrence also should be reported as suspected sabotage events as a precautionary measure.]** Specific reporting guidance for suspected sabotage events is presented below.

Power System Related Event or Activity

[When an event is determined to be suspected sabotage as described above, immediate notification should be made via the regional reporting procedures outlined in the Regional Emergency Notification System. The designated individual in the Emergency Notification System will notify the Regional 24-Hour Duty Officer/REO in accordance with regional reporting procedures. The Regional 24-Hour Duty Officer/REO will promptly notify the RDO. In addition, the Regional 24-Hour Duty Officer/REO will notify the Regional Special Agent. The RDO will immediately notify SSLE. Depending on the nature of the event, SSLE will provide prompt notification to the Office of the Chief Information Office (CIO). In the event the potential sabotage involves criminal activity, the Regional Special Agent will coordinate or conduct the investigation and provide guidance concerning preservation of evidence during restoration.

When the PRO determines the event may be suspected sabotage following review of the PO&M 172 Part I, the personnel making the determination will notify SSLE immediately. Depending on the nature of the event, SSLE will provide prompt notification to the Office of the CIO of any cyber related event analyzed by the PRO. In the event the potential sabotage involves criminal activity, the Regional Special Agent will coordinate or conduct the investigation and provide guidance concerning preservation of evidence during restoration.]

Electric System Coordination

To protect the BES, existing local notifications to interconnected partners regarding power operations and events should continue as defined in local

Standing Operating Procedures (SOP) and requirements. This excludes [**the reporting of suspected sabotage that requires additional analysis and will be reported by SSLE**.]

Cyber System-Related Event or Activity (SCADA, EACSS, etc.)

[Any unexplained event involving or affecting the normal operation of Reclamation computer systems is to be promptly reported to the Reclamation Enterprise Services Center (RESC), as detailed in the *BOR Computer Security Incident Response Handbook*.] Where possible, RESC personnel will follow their internal procedures to track and address the problem. [**The RESC personnel will promptly notify the RCSIRT as appropriate**.]

Unexplained events involving cyber systems suspected of being sabotage, including events related to supervisory control and data acquisition (SCADA) equipment used to operate or control Reclamation power facilities and/or Electronic Access Control and Surveillance System (EACSS) components used to monitor and control access to Critical Cyber Assets (CCAs), will also be reported via the guidelines provided in the *Power System Related Event or Activity* paragraph above. [**When actual sabotage is suspected or indicated, the RCSIRT will immediately notify SSLE.]**

Response

Prior to implementing any response activities, proper precautions should be taken by all parties to ensure the safety and security of the affected area, to preserve and protect evidence or a crime scene, and to possibly confirm the identity of any individuals responsible for the sabotage event.

Restoration

[Restoration of systems (including cyber systems), equipment, or processes directly impacted by a suspected sabotage event should be coordinated through the appropriate operating office, SSLE, and the CIO (if applicable).] Staff involved in restoration should be cognizant that any suspected sabotage event may have been initiated by deliberate means and that restoration efforts may be hampered or jeopardized by additional sabotage activities or planning.

Where practical, potentially sabotaged systems, equipment, or processes should not be restored until proper preliminary investigations have been concluded and evidence has been secured. Where emergency operating responsibilities exist that preclude the completion of preliminary investigation(s) prior to restoration, every

effort shall be taken to preserve as much information as practical while also addressing the safety of operating personnel, the public, and the facility.

Sabotage Reporting Follow-up Actions

Analysis of Information

[When an event is reported as suspected sabotage, SSLE and the RCSIRT (if appropriate) will conduct additional analysis of the information to determine if the event rises to the level of actual sabotage.] On behalf of the RCSIRT, the Office of the CIO will provide analysis of all suspected cyber sabotage events. SSLE will complete the analysis of all other events suspected of being caused by sabotage.

Internal Notification

[In the event SSLE concludes its analysis and finds that the event is not sabotage, SSLE will notify the appropriate Regional and Area Office Managers as to the results of the analysis.]

[If, as a result of investigation efforts, an event is confirmed to be sabotage, SSLE will notify the appropriate Regional and Area Office Managers.] This notification will potentially include any necessary sabotage response measures, including any recommended actions, in accordance with existing protocols used by operating personnel in the facility. If appropriate, cyber response guidance and local notifications will also be provided by the Office of the CIO.

Notification of Federal Law Enforcement

[If SSLE concludes an unexplained event is or appears to be sabotage, SSLE and the Regional Special Agent will immediately report it to the appropriate local Federal Bureau of Investigations (FBI) and the FBI Joint Terrorism Task Force. Where the unexplained event involves the tampering with, inappropriate use of, sabotage of, or abuse of cyber systems, the Office of the CIO will notify the U.S. Department of the Interior's Office of the Inspector General, and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) as appropriate and consistent with the *BOR Computer Security Incident Response Handbook*.]

External Notification of Sabotage

[SSLE is responsible for and will promptly report events related to the actual (confirmed) sabotage of power equipment or power-related facilities and

systems to the appropriate dispatching or security officials at the affected Electric Interconnected Partners.]

Attachment A
Sabotage Precursors and Indicators

An unexplained event or activity is considered to be reportable as potential sabotage. The following are provided as examples of potential sabotage activities.

A.1 Physical Sabotage Reporting Guidelines

- Any statement or belief by an employee or contractor that sabotage caused damage.
- Any incident involving explosives or incendiaries.
- Cases where there have been noticeable personnel issues in facilities and the affected systems are maintained or operated by those involved individuals.
- Any deliberate violation of any rule or procedure that leads to unit shutdown or damage.
- Suspicious discrepancies in log entries surrounding an incident, including annunciator, security, or entry logs.
- Any unexplained operation where sabotage is suspected.
- Unknown locks added to lockouts where sabotage is suspected.
- Misoperations or damage where no reasonable technical explanation is found.
- A pattern of accidental damage to equipment that appears beyond coincidental and/or the destruction or theft of equipment or system documentation.

A.2 Supervisory Control and Data Acquisition (SCADA) Sabotage Reporting Guidelines

- Any unexpected loss of control of the system, even temporarily.
- Any unauthorized modifications to systems, including outside connectivity issues, regardless of system status.
- Mis-wired SCADA connectivity to the plant - where such connections were previously okay and no change order is known to have been issued.
- Physically damaged SCADA wiring, either plant interface, SCADA power, network, or telecommunication, where the damage does not appear accidental.
- Any unauthorized downloading or uploading of information, connection to the internet or connection to another outside system.

- Cases where there have been noticeable personnel issues in facilities and the affected systems are maintained or operated by those involved individuals.
- Misoperations or damage where no reasonable technical explanation is found.
- Unaccounted for changes in software/firmware/hardware, including new or unexpected network or telephony connections (to include wireless access points).
- Discovery of unexpected user or operator accounts.
- Unexpected or spontaneous reboots of Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), main SCADA servers, or other SCADA equipment.
- Discovery of sensitive site-specific SCADA information on the Internet or Intranet (where such information was not known to be previously present).
- Unexplained or unexpected network traffic on the SCADA backbone.
- Unexplained or unexpected applications on SCADA servers, PLCs, RTUs, or other SCADA equipment.
- The destruction or theft of SCADA documentation.
- The detection of a “worm,” “virus,” or similar malware on a SCADA system.
- An obviously misdirected operation (attempts to control one device results in control of something else).
- An obviously misdirected indication (e.g., a status indication for one device is unexpectedly associated with another device instead).
- Unexpected equipment operation(s) that appear to be directed by the SCADA system—whether or not anyone was performing other operations at the same time.
- Obvious physical damage to SCADA equipment where the damage does not appear to be accidental.
- A pattern of accidental damage to SCADA equipment that appears beyond coincidental and/or the destruction or theft of SCADA documentation.

A.3 Electronic Access Control and Surveillance System Sabotage Reporting Guidelines

- Unexplained or spontaneous reboots of electronic security system equipment.

- Discovery of unexplained user or operator accounts on the electronic system.
- Other precursors and indicators as discussed in A.2 above.