


CYBER SECURITY INCIDENT RESPONSE PLAN

	* Category:	Critical Infrastructure Protection	
	Type:	Cyber Security	
	Document:	CIP-068	
	Owner:	James Kokotovich, Manager IT Support Services	
	Eff. Date/Rev. #	05/23/2012	014
	Approval:	John Miller, Network Security Architect Michael Pokas, Director IT Services	

* References to ITC are references to ITC Holdings Corp. together with all of its subsidiaries, unless otherwise noted.

1. INTRODUCTION

- 1.1. This document replaces CIP-068 Revision 013, dated 03/28/2012 and titled “Cyber Security Incident Response Plan.”
- 1.2. This document serves to satisfy the procedure requirements set forth in the following standards and will be reviewed annually as indicated by the associated Attachment 99 as described in GAP-001 Standard for Developing and Revising O&M Procedures:
 - 1.2.1. NERC Cyber Security Standard CIP-008 Requirement R1 through R2.
- 1.3. The purpose of this document is to define the annual testing process, and describe The Cyber Security Incident Response Plan steps used to effectively and efficiently manage a cyber-security incident by characterizing and classifying the event and the prescribed response actions and communication procedures to follow using the CIP-095 Incident Response and Asset Recovery Emergency Contact List. CIP-095 defines the Cyber Security Incident Response Team’s (CSIRT) roles and responsibilities and provides emergency contact information for the CSIRT and the Department of Energy (DOE) and ES-ISAC.

2. SCOPE AND RESPONSIBILITY

- 2.1. This process applies to all ITC employees, contractors, consultants, temporary employees and interns (referred to herein as ITC resources).
- 2.2. The CSIRT is responsible for responding to cyber security incidents.
- 2.3. Members of the CSIRT are identified in the CIP-095 Incident Response and Asset Recovery Emergency Contact List.
- 2.4. The Corporate Security Manager is responsible for determining whether local or national law enforcement agencies must be notified, in accordance with SEC-004 Sabotage Reporting.

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

- 2.5. The Senior Transmission System Coordinator (Sr. TSC) in the Operations Control Room is responsible for determining whether external operating entities must be notified.
- 2.6. This cyber security incident response plan must be tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the detailed review of a documented response of an actual incident.
- 2.7. All IT Services staff members must have access to a documented procedure that clearly specifies how cyber security incidents will be handled.
- 2.8. All relevant documentation related to reportable Cyber Security Incidents is retained for three calendar years. (CIP-008-3, R2)

3. REFERENCES

- 3.1. US Department of Energy – Form OE-417: Electric Emergency Incident and Disturbance Reporting: https://www.oe.netl.doe.gov/OE417_Form.aspx
- 3.2. ES-ISAC document Security Guideline for the Electricity Sector: Threat and Incident Reporting: www.nerc.com/files/Incident-Reporting.pdf
- 3.3. SEC-004 Sabotage Reporting
- 3.4. NERC Cyber Security Standard CIP-008
- 3.5. GAP-001 Standards for Developing Revising O&M Procedures
- 3.6. CIP-541 CIP Critical Asset and Cyber Asset List
- 3.7. CIP-542 Cyber Assets Used for Access Control or Monitoring of ESP or PSP
- 3.8. F1 – CIP-068 Cyber Security Incident Response Plan Checklist
- 3.9. CIP-095 Incident Response and Asset Recovery Emergency Contact List

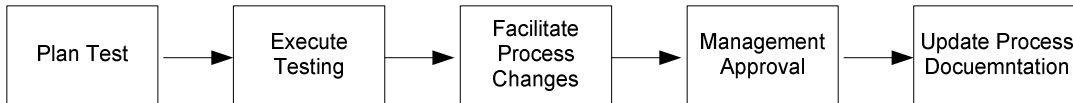
4. PRECAUTIONS

- 4.1. NA

5. PROCEDURE

- 5.1. **CSIRT Test Process**

CYBER SECURITY INCIDENT RESPONSE PLAN



5.2. Plan Testing (CIP-008-3, R1.6)

- 5.2.1. The CSIRT Team Lead (TL) or their CIP Compliance Analyst will plan the annual test of the Cyber Security Incident Response Plan.
- 5.2.2. The CSIRT TL will conduct a meeting with the members of the CSIRT and a determination is made regarding:
 - 5.2.2.1. The attack scenario(s) to include in the test.
 - 5.2.2.2. CSIRT members who will be involved in the testing process.

5.3. Execute Testing

- 5.3.1. The CSIRT conducts, at a minimum, a tabletop test of the incident response procedures.
- 5.3.2. Potential attack scenarios within the scope of testing could include:
 - 5.3.2.1. Malicious Code.
 - 5.3.2.2. Denial of Service Attack.
 - 5.3.2.3. Unauthorized Access.
 - 5.3.2.4. Equipment Theft.
 - 5.3.2.5. Social Engineering.
 - 5.3.2.6. Multiple Component Incidents.
- 5.3.3. A walk-through discussion of the selected attack scenario will be conducted by the CSIRT reviewing the process steps.
- 5.3.4. All process steps and response team actions are carefully evaluated to determine any improvements or adjustments that may be needed.

5.4. Facilitate Process Changes.

- 5.4.1. Plan improvements, corrections, or amendments identified during the testing process will be implemented by the CSIRT TL.
- 5.4.2. At the conclusion of the testing period a Test Track item will be logged to capture all CSIRT test activities.

5.5. Management Approval and Signature

- 5.5.1. Once testing of the Cyber Security Incident Response Plan is concluded and all required changes have been completed, the updated plan is submitted for approval to the CIP-068 Cyber Security Incident Response Plan document approvers. The Test Track log of

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

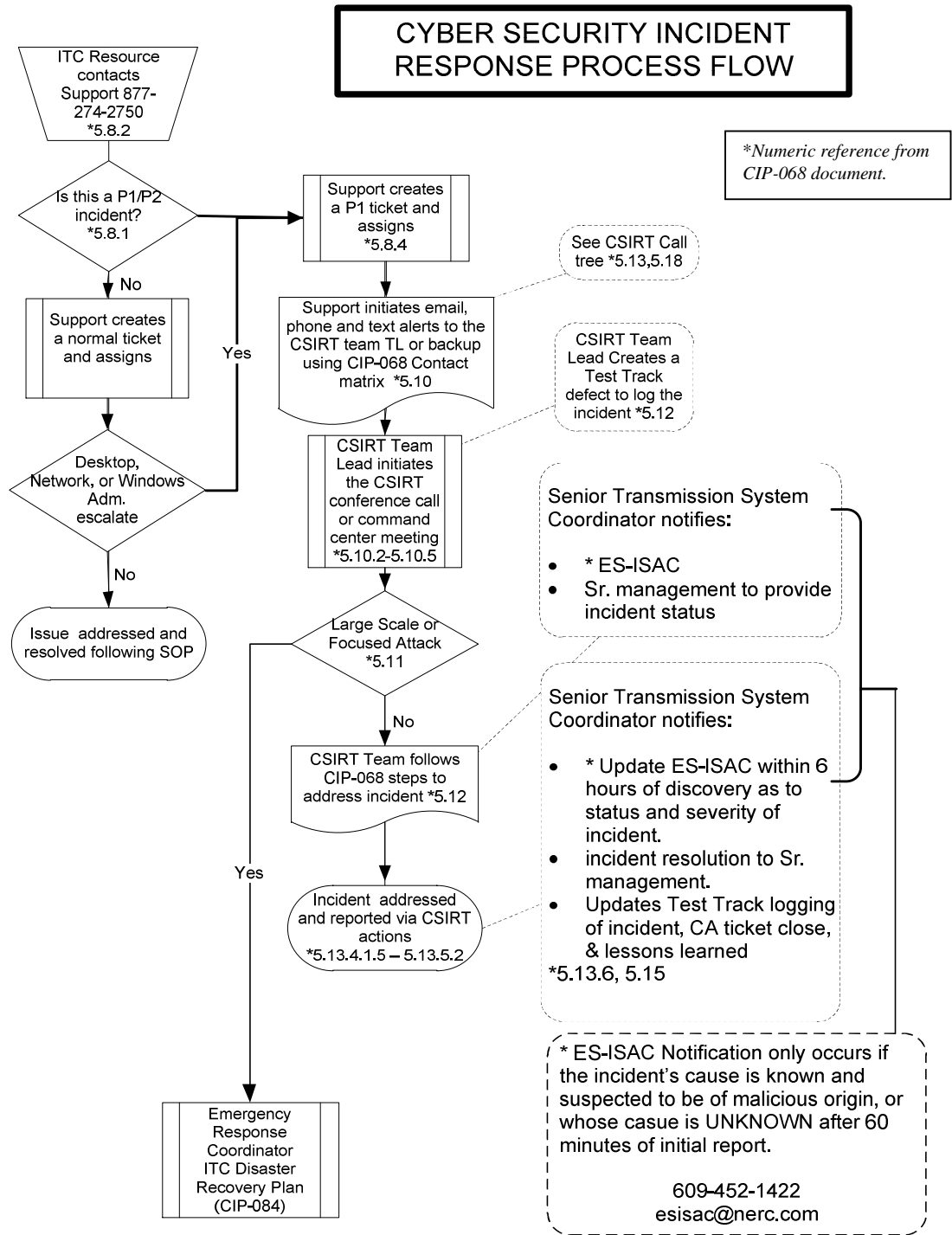
CYBER SECURITY INCIDENT RESPONSE PLAN

the Cyber Incident Response Plan will be reviewed and approved by the Director of IT Services as part of the Test Track approval workflow.

- 5.5.2. All changes to document CIP-068 Cyber Security Incident Response Plan must be implemented and documented within 30 days of the plan test by the CIP-008 standard owner.
- 5.6. **Update Documentation**
 - 5.6.1. Upon approval of the updated CIP-068 Cyber Security Incident Response Plan test, the document will be updated if improvements or changes are identified. The CSIRT Team Lead or his delegate will ensure that any necessary changes are incorporated. All changes will be logged in the document history.

CYBER SECURITY INCIDENT RESPONSE PLAN

5.7. INCIDENT RESPONSE PROCEDURE



PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
 Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

5.8. Incident Identification and Analysis

- 5.8.1. Any cyber security incident is defined as any malicious act or suspicious event that:
 - 5.8.1.1. Compromises, or was an attempt to compromise, the Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) of a critical cyber asset, or
 - 5.8.1.2. Disrupts, or was an attempt to disrupt, the operation of a critical cyber asset.
- 5.8.2. If an ITC resource experiences evidence of a cyber-attack or has suspicion that an attack is occurring, they should discontinue using the effected computing device immediately and take the following actions:
 - 5.8.2.1. Contact the IT Services help desk and report the incident.
 - 5.8.2.2. Document as much information as possible including:
 - 5.8.2.2.1. When was the suspicious activity first noticed.
 - 5.8.2.2.2. Systems or applications that may be compromised.
 - 5.8.2.2.3. Sensitive data stored within the compromised system.
 - 5.8.2.2.4. The data, equipment and/or property threatened.
 - 5.8.2.2.5. Describe any other pertinent details that may assist the CSIRT.
 - 5.8.2.3. Notify your immediate supervisor.
- 5.8.3. When a cyber-security incident is occurring or is suspected to be occurring, an incident ticket must be opened with the IT Services Helpdesk and the Helpdesk resource receiving the call must collect and enter the following information into the ticket to facilitate reporting needs:

CYBER SECURITY INCIDENT RESPONSE PLAN

- 5.8.3.1. Pertinent contact information of the reporting resource, including name, location, phone number, the date/time the incident was reported.
 - 5.8.3.2. Identify infrastructure that has been affected including the affected business systems, operating system, location, IP address and personnel involved.
 - 5.8.3.3. The nature of the cyber security incident, when it was first detected or suspected and the actual event that transpired to indicate a possible incident had taken place.
- 5.8.4. Under the following conditions the IT Service Helpdesk must be contacted immediately and a high priority incident (P1-P2) must be initiated when:
- 5.8.4.1. Anti-virus software sends three alerts for the same virus within a thirty minute period, or any virus is detected on a device that is listed on CIP-541 or CIP-542.
 - 5.8.4.2. Suspicious entries in network logs from firewalls and routers are discovered by a member of the IT Services.

5.9. Incident Analysis

- 5.9.1. From the above conditions SME's will analyze the incident and make a determination whether the incident should be classified as a CSIRT incident. (One that requires DOE and ES-ISAC notification).
 - 5.9.1.1. If it is determined, based on the criteria listed in 5.13.5 that DOE and ES-ISAC should be contacted, then the SME will contact the IT Services Helpdesk to escalate the incident, and initiate the CSIRT process.
 - 5.9.1.2. If it is determined, based on the criteria listed in 5.13.5 that DOE and ES-ISAC should not be contacted, the incident will be handled based on standard operating procedures for operational incidents.

5.10. Notify Incident Response Team

- 5.10.1. The IT Services Helpdesk will immediately notify the CSIRT TL, and the TL backup via phone call, and text messaging to initiate the CSIRT communication plan.

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

5.10.2. CSIRT TL or TL backup will initiate the CSIRT conference call and include the conference phone number and access code in the alerts sent out to the CSIRT TL, and TL back-up.

5.10.3. The communication from the IT Services Helpdesk to the above individuals will include the conference call number and access code and the message:

“CSIRT ALERT!! Call IMMEDIATELY!!”

5.10.4. Once the conference call is initiated, the CSIRT TL or TL back-up contact other resources from the CSIRT as needed to assist in addressing the incident.

5.10.5. The CSIRT TL will facilitate the communication to the appropriate ITC senior management team members as appropriate. At a minimum the CSIRT TL will notify and provide status updates to the Director of IT Services.

5.11. Characterize and Classify Event (CIP-008-3, R1.1)

5.11.1. The CSIRT TL will direct the team members where to convene and what next steps will be needed to address and resolve the incident.

5.11.1.1. CSIRT resources contact information, roles and responsibilities are listed in the CIP-095 Incident Response and Asset Recovery Emergency Contact List . Appropriate resources will be assigned to assess the nature of the attack and its potential impact.

5.11.1.2. In order to determine the potential impact of the incident and select the appropriate response strategy, the following factors must be considered and/or identified:

5.11.1.2.1. Determine if the event is real incident or perceived.

5.11.1.2.2. Is the security incident still in progress?

5.11.1.2.3. Systems or applications that have been compromised.

5.11.1.2.4. What sensitive data is stored on the compromised system?

5.11.1.2.5. The data, equipment and/or property threatened.

5.11.1.2.6. Where do the assets in question reside on the network?

CYBER SECURITY INCIDENT RESPONSE PLAN

- 5.11.1.2.7. The entry point of the attack (i.e. fence, gate, doorway, network, internal, internet, phone line, etc.).
- 5.11.1.2.8. Immediate and long term impact to ITC.
- 5.11.1.2.9. How quickly can the attack be contained?
- 5.11.1.3. Based on the identified attack type(s), the CSIRT will select and execute the appropriate response strategy within section 5.12 Incident Handling Procedures and Response Actions.
- 5.11.2. The CSIRT will update the incident ticket as information becomes known, including impact on critical infrastructure, expected duration of impact or time to restore and suspected root cause.

5.12. Incident Handling Procedures and Response Actions (CIP-008-3, R1.2)

- 5.12.1. **Malicious Code:** A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
 - 5.12.1.1. Evaluate the origin and severity of the attack.
 - 5.12.1.2. Document the resources or systems that have been affected and estimate the current and potential effect.
 - 5.12.1.3. Disconnect infected systems from the network and block all transmission mechanisms for the malicious code.
 - 5.12.1.4. Mitigate the vulnerabilities exploited by the malicious code.
 - 5.12.1.5. Perform evidence preservation procedures as soon as possible.
 - 5.12.1.6. Disinfect, quarantine, delete and/or replace infected files.
 - 5.12.1.7. If it is determined that damage has resulted from the attack take the necessary action to resolve the incident and recover from the damage.
 - 5.12.1.8. Recovering from the damage incurred could include, but is not limited to, patch application, system upgrades, system or application reinstallation, or data recovery.
 - 5.12.1.9. Recover affected systems to an operationally ready state.
 - 5.12.1.10. Monitor the systems affected to ensure systems are functioning normally and that the attack has been successfully contained and the threat eliminated.

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

- 5.12.1.11. Use Test Track to completely document the incident including a copy of the malicious code and all containment efforts, communications actions, resolution procedures and recovery actions (in reference to CIP-084 Asset Recovery Process).
- 5.12.2. **Denial of Service Attack:** An attack that prevents or impairs the authorized use of networks, systems, or applications by overloading and/or exhausting resources.
 - 5.12.2.1. Evaluate the origin and severity of the attack and identify the host perpetrating the attack.
 - 5.12.2.2. Note the resources or systems that have been affected and forecast which resources will be affected.
 - 5.12.2.3. Block the host perpetrating the attack and shut down all network access to the offending systems.
 - 5.12.2.4. Perform evidence preservation procedures as soon as possible.
 - 5.12.2.5. If it is determined that any damage has occurred as a result of the DoS attack, then take necessary action to resolve the incident and recover from the damage.
 - 5.12.2.6. Eliminate the vulnerabilities that allowed the attack to occur.
 - 5.12.2.7. Recover affected systems to an operationally ready state.
 - 5.12.2.8. Monitor the systems affected to ensure normal functionality and that the attack has been successfully contained and the threat eliminated.
 - 5.12.2.9. Use Test Track to completely document the incident including a copy of the malicious code and all containment efforts, communication actions, resolution procedures and recovery actions (in reference to CIP-084 Asset Recovery Process).
- 5.12.3. **Unauthorized Access:** Gaining logical or physical access without permission to a network, system, application, data, or other resource.
 - 5.12.3.1. Determine if the origin of the incident is internal or external and the type of access breach that is occurring.
 - 5.12.3.2. Document the resources or systems that have been affected and estimate current and potential technical affect.
 - 5.12.3.3. Lock the account out and log it out of the network server.

CYBER SECURITY INCIDENT RESPONSE PLAN

- 5.12.3.4. Determine if containment was sufficient or if there are signs of intrusion elsewhere in the system's environment.
 - 5.12.3.5. Perform evidence preservation procedures as soon as possible.
 - 5.12.3.6. If damage has occurred as a result of the unauthorized access attack, take required action to resolve the incident and recover from the damage.
 - 5.12.3.7. Eliminate the vulnerabilities that allowed the attack to occur.
 - 5.12.3.8. Recover affected systems to an operationally ready state.
 - 5.12.3.9. Monitor the systems affected to ensure normal functionality and that the attack has been successfully contained and the threat eliminated.
 - 5.12.3.10. Use Test Track to completely document the incident including a copy of the malicious code and all containment efforts, communication actions, resolution procedures and recovery actions (in reference to CIP-084 Asset Recovery Process).
- 5.12.4. **Equipment Theft:** The theft of mobile computing equipment including laptop computers, smart phones, PDA's, etc.
- 5.12.4.1. **Laptop computing equipment.**
 - 5.12.4.1.1. Disable the user account.
 - 5.12.4.1.2. Determine exposure due to confidential, sensitive, or proprietary information resident on the equipment.
 - 5.12.4.1.3. Alert the Physical Security Manager of the attack and notify the department supervisor.
 - 5.12.4.2. **Smart Phone devices (ie. I-Phones, Blackberry's).**
 - 5.12.4.2.1. Remotely lock the device and cleanse the device of all data.
 - 5.12.4.2.2. Alert the Corporate Security Manager of the attack and notify the department supervisor.
 - 5.12.4.2.3. The Corporate Security Manager will contact appropriate law enforcement agencies if necessary.
 - 5.12.4.3. Use Test Track to completely document the incident including a copy of the malicious code and all containment

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

efforts, communications actions, resolution procedures and recovery actions (in reference to CIP-084 Asset Recovery Process).

- 5.12.5. **Social Engineering:** Manipulating people into performing disclosure actions or divulging confidential information.
 - 5.12.5.1. Determine the scope of the attack and facilitate communications to the appropriate resources.
 - 5.12.5.2. Alert the Corporate Security Manager of the attack and notify the department supervisor.
 - 5.12.5.2.1. The Corporate Security Manager will contact appropriate law enforcement agencies if necessary.
 - 5.12.5.3. Notify the ITC senior management representatives as appropriate.
 - 5.12.5.4. Notify the ITC user base and alert them to the nature of the attack.
- 5.12.6. **Multiple Component Incidents:** Multiple Component Attacks: A single incident that encompasses two or more components.
 - 5.12.6.1. Evaluate the origin and severity of the attack.
 - 5.12.6.2. Document the resources or systems that have been affected and estimate current and potential technical affect.
 - 5.12.6.3. If an external attack then shut down the VPN routers and firewalls.
 - 5.12.6.4. Disconnect infected systems from the network.
 - 5.12.6.5. Perform evidence preservation as soon as possible.
 - 5.12.6.6. Determine any damage that may have resulted from the attack.
 - 5.12.6.7. If damage has occurred as a result of the incident, take required action to eradicate the incident and recover from the damage.
 - 5.12.6.8. Recover affected systems to an operationally ready state.
 - 5.12.6.9. Monitor the systems affected to ensure normal functionality and that the attack has been successfully contained and the threat eliminated.

CYBER SECURITY INCIDENT RESPONSE PLAN

5.12.6.10. Use Test Track to completely document the incident including a copy of the malicious code and all containment efforts, communications actions, resolution procedures and recovery actions (in reference to CIP-084 Asset Recovery Process).

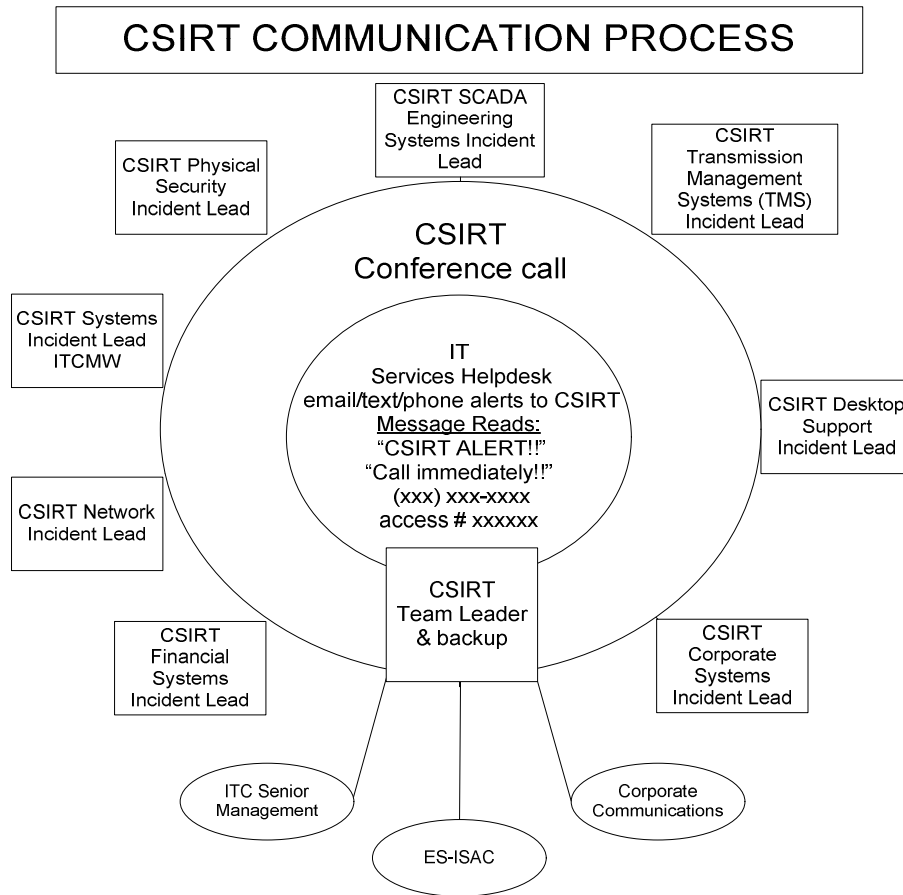
5.13. Communication Plan (CIP-008-3, R1.2 and R1.3)

5.13.1. During the course of a P1-P2 cyber security incident the following communication plan will be in used:

5.13.2. This plan becomes a CSIRT incident if and when it becomes necessary to contact DOE and ES-ISAC.

5.13.3. This diagram indicates the roles that can be called upon by the CSIRT TL to help resolve an incident.

5.13.4. Communication Plan Diagram



PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

5.13.4.1. When a P1-P2 incident analysis causes technicians to contact the Helpdesk to escalate to a CSIRT incident:

- 5.13.4.1.1. The IT Services Helpdesk lead is responsible for setting up a conference bridge call, calling and texting the CSIRT TL and his backup.
- 5.13.4.1.2. Alert notices will be sent out via text and phone calls. Phone calls will persist until each CSIRT TL and his backup are reached.
- 5.13.4.1.3. The alert will include a message stating “CSIRT ALERT” Call IMMEDIATELY”. And will include the conference call phone number and access code number for respondents to use upon receipt of the alert.
- 5.13.4.1.4. The CSIRT TL or his backup will take ownership of the incident and ensure that the incident is addressed and brought to resolution.
- 5.13.4.1.5. The CSIRT TL will retain primary responsibility for coordinating communication between the CSIRT members and the rest of the IT organization, senior ITC management and the corporate communications lead.
- 5.13.4.1.6. The CSIRT TL will notify the ITC senior management and other ITC resources as necessary.
- 5.13.4.1.7. The CSIRT TL will alert the Corporate Security Manager or Security Command Center of the attack. Corporate Security will perform notifications to external law enforcement agencies in accordance with their procedures if appropriate for the incident.
- 5.13.4.1.8. The CSIRT TL will alert the Sr. TSC in the Operations Control Room (OCR). The OCR will perform notifications to external operating entities in accordance with their procedures if appropriate for the incident.
- 5.13.4.1.9. The Sr. TSC (or designate) will perform notification to the DOE and ES-ISAC as

CYBER SECURITY INCIDENT RESPONSE PLAN

described in section 5.13.5., if appropriate for the incident.

- 5.13.4.1.10. The CSIRT TL will facilitate ongoing communication to ITC senior management at regular intervals for the duration of the incident.

5.13.5. When to Notify DOE and ES-ISAC

5.13.5.1. DOE and ES-ISAC reporting should be performed in accordance with the guidelines set forth in the Electric Emergency Incident and Disturbance Report (OE-417) and ES-ISAC document Security Guideline for the Electricity Sector: Threat and Incident Reporting.

5.13.5.2. An initial report to provide notice that an incident has occurred is required within 60 minutes of detection of an incident. This report should be provided even if the exact nature is not yet determined. Within 6 hours after submittal of the initial report, a follow-up report shall be provided when more complete information is generally known. A final report for confirmed malicious events only shall be submitted within 60 days and will contain all relevant facts that can be determined regarding the incident.

5.13.6. Incident Criteria Mandating DOE and ES-ISAC Reporting

- 5.13.6.1. Cyber security incidents or threats meeting the following criteria whose cause is known or suspected to be of malicious origin, or whose cause is unknown after 60 minutes from the initial incident discovery must be reported to the DOE and ES-ISAC. Contact DOE and ES-ISAC using the CIP-095 Incident Response and Asset Recovery Emergency Contact List
- 5.13.6.2. Loss of a substation identified as a CIP critical asset or loss of any substation $\geq 230\text{kV}$ lasting 60 minutes or longer.
- 5.13.6.3. Loss of interconnection tie line(s) to external transmission owners $\geq 230\text{kV}$ lasting 60 minutes or longer. When a cyber-security incident is occurring or is suspected to be occurring, an IT Services Helpdesk ticket must immediately

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

- be opened and will be used to help capture incident information for later reporting in Test Track.
- 5.13.6.4. Loss of power to the operations control center lasting 30 minutes or longer.
 - 5.13.6.5. Unanticipated loss of a load center $\geq 200\text{MW}$ lasting for 30 minutes or longer.
 - 5.13.6.6. Loss of critical telecommunications, including telemetry, essential to system operations lasting for 30 minutes or longer.
 - 5.13.6.7. Anomalous or non-characteristic transmission system behavior lasting for 30 minutes or longer.
 - 5.13.6.8. Announced and credible threats that, in ITC's judgment, would significantly impact transmission system operations if carried out successfully.
 - 5.13.6.9. Any unauthorized, highly focused and concerted Cyber attempts against, or intrusions into, systems capable of impacting real time control and operation of the transmission system.
 - 5.13.6.10. Any outside or unauthorized inside attempts to extract sensitive or proprietary information from employees that, in ITC's judgment, could aid in planning or executing cyber intrusions that could impact transmission system operations.
 - 5.13.6.11. Activities such as unauthorized downloading, transferring, planting or pre-positioning malicious code, viruses or computer/network exploit tools that could affect transmission system operations.
 - 5.13.6.12. No ES-ISAC report should be submitted when it is known with certainty that the cause is not of malicious origin.
- 5.13.7. The following information will be reported to the OE-417 – Electric Emergency Incident and Disturbance Report and ES-ISAC using the ES-ISAC "Threat and Incident Report Form:"
- 5.13.7.1. Date, time and location of the incident; brief description of the incident; impact of critical infrastructure, public health and safety, environment; expected duration of impact or time to restore; root cause, if known; reporting individual, company and contact information; law enforcement involvement, if any.

5.14. Evidence Preservation

- 5.14.1. Back-ups of the compromised systems should be performed if required and feasibly possible.
 - 5.14.1.1. Back-ups should be facilitated using new storage media.
 - 5.14.1.2. Document information regarding the back-ups including who backed up the systems, what time the backups occurred, how they were secured, and which resources had access to them.
 - 5.14.1.3. If possible, these back-up copies should be taken prior to any system restore procedures being executed.
 - 5.14.1.4. Once created, store back-ups in a physically secure location and new disks should be used to restore the systems.
 - 5.14.1.5. Back-up copies will be used as forensic evidence in the event of the prosecution of an attacker.

5.15. Lessons Learned

- 5.15.1. The CSIRT TL will convene a “post mortem” meeting with the CSIRT team and appropriate ITC management resources within ten business days of the incident resolution to review the following details of the cyber security incident or breach:
 - 5.15.1.1. Response actions, containment, communication and recovery procedures.
 - 5.15.1.2. Determining if the incident caused damage before it was detected.
 - 5.15.1.3. How well the team adhered to established incident response policies and procedures.
 - 5.15.1.4. Determine if the actual cause of the incident was identified.
 - 5.15.1.5. Identifying measures, if any, that could have prevented the incident.

CYBER SECURITY INCIDENT RESPONSE PLAN

5.15.1.6. Review actions by CSIRT team members and identify gaps and/or areas for improvement.

5.15.2. The CSIRT TL will ensure that all pertinent information related to the cyber security incident is logged in Test Track.

5.15.3. The CSIRT TL will ensure that any recommended changes or improvements to the process and/or policy are also recorded in the incident log in Test Track.

5.15.4. The CSIRT TL will log lessons learned, which will include: meeting notice(s), agenda, minutes and recommended changes or improvements into Test Track.

5.16. Update Process Documentation (CIP-008-3, R1.4)

5.16.1. Recommendations and/or changes captured as a result of the lessons learned meeting are incorporated into the CIP-068 document by CIP Compliance Analyst within thirty calendar days of discovery.

5.16.2. The Director of IT Services will review process changes with the members of the CSIRT and conduct training and testing exercises as necessary.

5.17. Annual Documentation Review (CIP-008-3, R1.5)

5.17.1. ITC document GAP-001 describes the Attachment 99 review process that is followed to review all CIP policies annually.

5.17.2. If there are no changes or updates required, this will be indicated within document history.

6. ATTACHMENTS

6.1. CIP-068 Att99 Annual Review Internal-Attachment 99

7. MISCELLANEOUS

7.1. Definitions

7.1.1. High Priority Incident (P1-P2):

Incident Priority	Business Impact
-------------------	-----------------

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

Incident Priority	Business Impact	
P1 (Critical)	<p>An Incident affecting a business critical application or that affects a high number of Authorized Users and for which a delay in restoration of service is not acceptable.</p> <p>An outage or a major loss of functionality of a business critical application.</p> <p>Illustrative examples of P1 Incidents include:</p> <p>A major loss of functionality affecting online software or batch commitments</p> <p>Multiple applications and/or business units affected (for example, the loss of an entire cluster or a production database supporting multiple applications)</p> <p>Loss of a network component (or other equipment failure) that has a major impact to business functions impacting large Workgroups and/or multiple sites.</p> <p><i>Note: Initial reporting of P1s MUST be via direct telephone Contact and confirmed. Additional information may be provided by non-voice methods.</i></p>	
P2 (High)	<p>An Incident affecting a business important application or a high number of Authorized Users and for which a delay in restoration of service is not acceptable.</p> <p>Illustrative examples of P2 Incidents include:</p> <p>Potential major loss of functionality affecting online software or batch commitments, for which preventive action must be taken immediately to prevent an outage</p> <p>A major loss of functionality affecting online software for a single application, a single business unit, or multiple small Workgroups</p> <p>A partial workaround or bypass is available, but functionality remains materially degraded</p>	
Incident Priority	Response Time	Restoration of Service
P1 (Critical)	Within 15 minutes, 85% of the time (7x24x365)	Within 2 hours, 80% of the time (7x24x365)
P2 (High)	Within 1 business hour, 85% of the time	Within 4 business hours, 80% of the time

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

8. APPROVALS

Owner: _____ <Signature on file> Date: 05/16/2012

Approver: _____ <Signature on file> Date: 05/16/2012

Approver: _____ <Signature on file> Date: 05/16/2012

9. REVISION HISTORY

Effective Date	Revision Number	Individual Making Edits	Reason / Comments
06/25/08	000	M. Pokas	Initial documentation
8/11/08	001	R. Gilmore	Addition of 5.2.1.2.3 per L. Trammer & M. Pokas.
9/2/2008	002	R. Gilmore	L. Trammer: Made edits based on Lessons Learned from 8/16/08 incident review. Added reference to 3.1, updated 3.2, and rewrote section 5.8.2 per Beth Howell.
06/30/09	003	M. Pokas	Restructured the document based on the annual review. Changed from SSE to CIP. Add NERC reference in Section 1.2 and Attachment 99.
10/28/09	004	M. Pokas	Added a statement to indicate that changes resulting from lessons learned must be implemented within 90 calendar days.
11/24/09	005	R. Scheels	Added Section 2.7 – Cyber Security Incidents may result in Disaster Recovery Plan entry conditions.
03/31/10	006	A. Stefan	Section 1.2: Changed “periodically” to “annually”. Section 5.9.4.2: Changed from 90 to 30 calendar days. Section 6: Added “tt” to A”tt”99.

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

07/16/10	007	M. Ensink	<p>Section 3 - Added document CIP-083, ITC Incident Response Lessons Learned Form and ITC Incident Report Form.</p> <p>Section 5.2.5 - Added IT Services and 'if one has not already been opened'.</p> <p>Section 5.3.1 Added reference to CIP-568 and added verbiage about their respective roles.</p> <p>Section 5.4.1.1 - Added roles and responsibilities and doc CIP-568 reference.</p> <p>Section 5.4.2 -Removed 'help desk'.</p> <p>Section 5.6.1.4.4 - Changed section reference from 5.8 to 5.7.</p> <p>Section 5.7.3 - Changed collecting to collects.</p> <p>Section 5.7.5 - Changed reporting to reported and added ES-ISAC to form name.</p> <p>Section 5.8 - Changed 'as soon as' to 'if required and'.</p> <p>Section 5.9.4 - Added for lessons learned.</p> <p>Section 5.2.3.1 - Removed department and email address.</p> <p>Replaced IT infrastructure team with IT Services throughout document.</p> <p>Replaced incident ticket with IT Services help desk ticket throughout.</p> <p>Section 5.2.4.4 - Added 'systems' to suspicious network.</p> <p>Section 5.3.2 - Added 'or other resources'.</p> <p>Section 5.4.1.2 - Replaced determined with considered.</p> <p>Replaced resume with recover in sections 5.5.1.9, 5.5.3.8, and 5.5.6.8.</p> <p>Section 5.9.5.2 - Added 'and documented'.</p>
----------	-----	-----------	--

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

12/17/10	008	C.Lewis	<p>Changed document ownership from Mike Pokas, Director of IT Services to John Miller, Network Security Architect Added Mike Pokas, Director of IT Services to the approvers.</p> <p>Section 1.1: Consolidated CIP-069 and CIP-568 into CIP-068 felt these could all be in one document. As a result section 5 now contains the content from CIP-069 and section 6 has original content from CIP-068 and section 5.16 has content from CIP-568. Section 1.3 changed to incorporate the purpose of CIP-069.</p> <p>All references to Manager of Information Security and IT Governance changed to Director of IT Services; CSIRT Team Lead changed to principal leader and coordinator of the process changed from Director of IT Services.</p> <p>Section 5.16 Added PR, ESISAC, and IT Media Lead to R&R Matrix, added text addresses and email addresses to R&R Matrix</p> <p>Changed or added sections 5.4.2, 5.5.1, 5.11.1.10, 5.11.2.9, 5.11.3.10, 5.11.4.3, 5.11.6.10, 5.12.4.2, 5.14.2, 5.14.3, 5.14.4. such that the audit trail process no longer uses printed and signed forms: CIP-068-F1, CIP-068-F2 and CIP-069-F1 to record incidents, lessons learned from incidents or incident testing, respectively, to using the Test Track workflow within the IT Services Change Management project of the application..</p> <p>Section 5.1 Test process flow diagram changed from “Initiate Testing” to “Plan Test”</p> <p>Section 5.12.2 added CSIRT communication plan diagram</p> <p>Section 5.7 added a diagram of the Cyber Security Incident Response Procedure and the Cyber Security Incident Response Process Flow diagram</p>
----------	-----	---------	--

CYBER SECURITY INCIDENT RESPONSE PLAN

05/25/11	009	A. Cook	<p>Section 1.2 – Added GAP-001. References Section: Added GAP-001 Standards for Developing Revising O&M Procedures Throughout document replaced “his delegate” with “CIP Compliant Analyst” Section 5.8.4. Replaced CSIRT with IT Service Helpdesk. Added “high severity/impact” and “when,” deleted “report.” Section 5.8.4.1. Reworded so it now states, “Anti-virus software sends three alerts for the same virus within a thirty minute period or any virus detected on a device that is listed on a CIP-541 or CIP-542. Deleted Section 5.8.4.2. per John Miller’s request. Inserted section 5.9. Incident Analysis. Added sub-bullet 9.1.1.stating, “From the above conditions, SME’s will analyze the incident and make a determination whether the incident should be classified as a CSIRT. Added 9.1.1.1. stating, “If it is determined, based on the criteria listed in 5.13 that ES-ISAC should be contacted, then the SME will contact the IT Services Helpdesk to escalate the incident, and initiate the CSIRT process. Added 9.1.1.2., which states, If it is determined, based on the criteria listed in 5.13 that ES-ISAC should not be contacted, then the incident will be handled based on standard operating procedures for operational incidents Revised Section 5.9.2. to state, “...alerts sent out to the CSIRT team lead, team lead back-up, and the IT Services Delivery Manager.” Revised section 5.10.2.1. stating, “The communication from the IT Services Helpdesk to the above individuals will include, “CSIRT ALERT!! Call IMMEDIATELY!!” Revised section 5.9.3. to state, “Once the conference call is initiated, the CSIRT team lead, team lead back-up, and the IT Services Delivery Manager contact other resources from the CSIRT as needed to assist in addressing the incident. To section 5.14.1. added “within 48 hours of incident”</p>
----------	-----	---------	---

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

05/25/11	009 (Con"t)	A. Cook	<p>Section 5.14.4. Added "which will include: meeting notice(s), agenda minutes." Changed 5.15.1 to 10 business days Added 5.17 Annual Documentation Review. Also, added sub-bullet 5.17.1. stating, "ITC document GAP-001 describes the Attachment 99 review process that is followed to review all CIP policies annually." 5.19 Added Mike Swanson as CSIRT Network Incident Lead and moved Jeff Weiner to backup. Removed Akram Saeed as backup. 5.19 Replaced Kevin Madis with Grant Bainbridge for CSIRT Systems Incident Lead ITCMW</p>
07/19/11	010	C. Lewis D. Bates	<p>Added C. Lewis as an approver. Added Section 2.7 back in. It was accidentally removed from rev. 009 (in rev 008 is was Sec. 2.8) Added Sec. 3.5,-3.7 Added "protective relays" to the scope of responsibility for the CSIRT SCADA Engineering Systems Incident Lead to accommodate the 800+ CCAs added to CIP-541.</p>

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
 Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

10/27/11	011	A. Cook	<p>Replaced Jeff Weiner with Kevin Madis as CSIRT Incident Network Lead (and all contact information).</p> <p>Replaced Kevin Madis with Grant Bainbridge as CSIRT Systems Incident Lead ITCMW (and all contact information).</p> <p>Replaced Dave Bates with James Kokotovich as SCIRT ciber Primary Incident Lead (and all contact information).</p> <p>Replaced Henry Oyier with Diana Yang as CSIRT Desktop Support Incident Lead – primary contact. Also replaced Dave Bates as secondary contact with Kevin Bartlett (and all contact information).</p> <p>Added James Kokotovich, IT Operations Manager as back up to CSIRT Team Lead and removed Chuck Lewis.</p> <p>Replaced James Kokotovich as primary CSIRT Key IT Contact with Chuck Lewis (and all contact information).</p> <p>Section 3.1 Updated web address from http://www.esisac.com/library-guidelines.htm to www.nerc.com/files/Incident-Reporting.pdf as old address was inactive.</p> <p>Flow Chart: 1) Added Numeric references (signified with *) from within CIP-068 to process flow chart, as well as key. 2) Also updated 1st decision box from “Does this Incident match CSIRT scenario” to “Is this a P1/P2 incident? 3) Updated decision box to reflect support contacting CSIRT TL or backup, not CSIRT.</p> <p>Section 5.10.2 – Updated IT Services Help Desk to CSIRT TL or TL backup to initiate CSIRT communication.</p> <p>Section 5.11.1.3 updated handling procedure reference from 6.4 to 5.12.</p>
----------	-----	---------	--

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

02/22/12	012	A. Cook	<p>Communication Matrix: Updated John Mooney from CSIRT Network Incident Lead Resource to Back-up and Kevin Madis from Back-up to Lead Resource. Updated Diana Yang from CSIRT Desktop Support Lead Resource to Back-up and Kevin Bartlett from Back-up to Lead Resource. Updated CSIRT Corporate Systems Incident Lead from Corey Muylaert to Paul Leslie, TechOps Engineer. Updated Pedro Melendez title from Principal Engineer, SCADA to Senior Staff Engineer, SCADA.</p>
03/28/12	013	A. Cook	<p>Added F1 - CIP-068 Cyber Security Incident Response Plan Checklist. Added CIP-008 standard and requirement references throughout document where applicable. Added US Department of Energy references wherever ES-ISAC reporting noted. Section 3: Included US DOE OE-417 Form to References. Also, added F1-CIP-068 CSIRT Checklist. Section 5.12 Added reference to CIP-084 Asset Recovery Process where asset recovery process referenced. Section 5.12.4 and 5.12.5 updated Blackberries to include all smartphones. Updated example list. Section 5.12.4.2.2 Updated Physical Security Manager to Corporate Security Manager. Section 5.13.4.1.8 Updated to reflect Transmission System Coordinator Lead (or designate) to perform notification of cyber security incident to DOE and ES-ISAC. Section 5.18 Updated CSIRT Team Lead backups: Removed C. Lewis. Added Kevin Madis and Akram Saeed. Also, updated grid with DOE emergency contact information. Removed 5.18 CSIRT Communication Matrix as it has been separated into its own document – CIP-095 Incident Response and Asset Recovery Emergency Contact List. Updated all sections with information pertaining to this reference. Updated John Miller with James Kokotovich as Document Owner and replaced Charles Lewis with John Miller as an Approver.</p>

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed

CYBER SECURITY INCIDENT RESPONSE PLAN

05/23/12	014	K. Madis	<p>Section 1.3: Replaced references to Cyber Security Incident Response Roles and Responsibility matrix with CIP-095 Incident Response and Asset Recovery Emergency Contact List.</p> <p>Section 2.5. Established abbreviation Senior Transmission System Coordinator to (Sr. TSC) and removed reference to EMR-007.</p> <p>Section 3.4: Removed EMR-007 Electric Emergency Incident Notifications from reference documents.</p> <p>Section 5.5.2: Added that the CIP-008 standard owner will update CIP-068 within 30 days of the plan test.</p> <p>Diagram 5.7: Senior Transmission System Coordinator replaces CSIRT Team Lead for contacting ES-ISAC.</p> <p>Sections 5.13.4.1.8-9: Updated to reflect Sr. TSC abbreviation</p> <p>Section 7.1: Added definition for High priority incident (P1-P2).</p>
----------	-----	----------	--

PROPRIETARY, CONFIDENTIAL OR PRIVILEGED INFORMATION
Verify Current Version Prior to Use — Uncontrolled When Printed