

Summary of M-13 Rev. 66 Changes

Dean Manno
SOS-Joint meeting
September 6th, 2018

Overview of Changes:

- Cover to Cover Periodic Review
- Section 3.2 added “Production System Freeze Change” to Conservative Ops
- Section 3.3 corrected formatting for Day-Ahead commitment instructions
- New Section 3.5 added for “Long Duration Extreme Weather”
 - Old Sections 3.5, 3.6, 3.7, and 3.8 renumbered accordingly
- Section 3.6 added language for disabling auto-reclose
- Section 4.1 deleted Exhibit 4 table
 - Former Exhibit 4 content reformatted and inserted into existing section 4.1 and new sections 4.3 and 4.4
- New section 4.3 for PJM operational procedure for physical threats
- New section 4.4 for PJM operational procedure for cyber threats against PJM
 - New section 4.4.1 for loss of ICCP or EMS capabilities operational procedure
 - New section 4.4.2 for loss of internet operational procedure
 - New section 4.4.3 for loss of all telecommunications operational procedure
- New section 4.5 for PJM operational procedure for cyber threats against member company
- New section 4.6 for PJM operational procedure for High-Altitude Electromagnetic Pulse
- Section 6.4 added language to adjust “Resource Limited Unit” reporting time-frame and minimum run time requirements to place additional Fuel Limited Resources into the Maximum Emergency Category during long duration extreme weather events.

- Contact Dean Manno (dean.manno@pjm.com) with questions
- Continue first reads at September OC and MRC meetings
- Second read (and request for endorsement) scheduled for October SOS-Joint meeting

- Reviewing operator training impacts of Manual changes

Appendix

- Section 3.2 added “Production System Freeze Change” to Conservative Ops

- **PJM issues a Production System Change Freeze: PJM will refrain from updating any business application systems, programs, data, systems software, hardware and any other aspect of the information-processing environment at PJM**

Note:

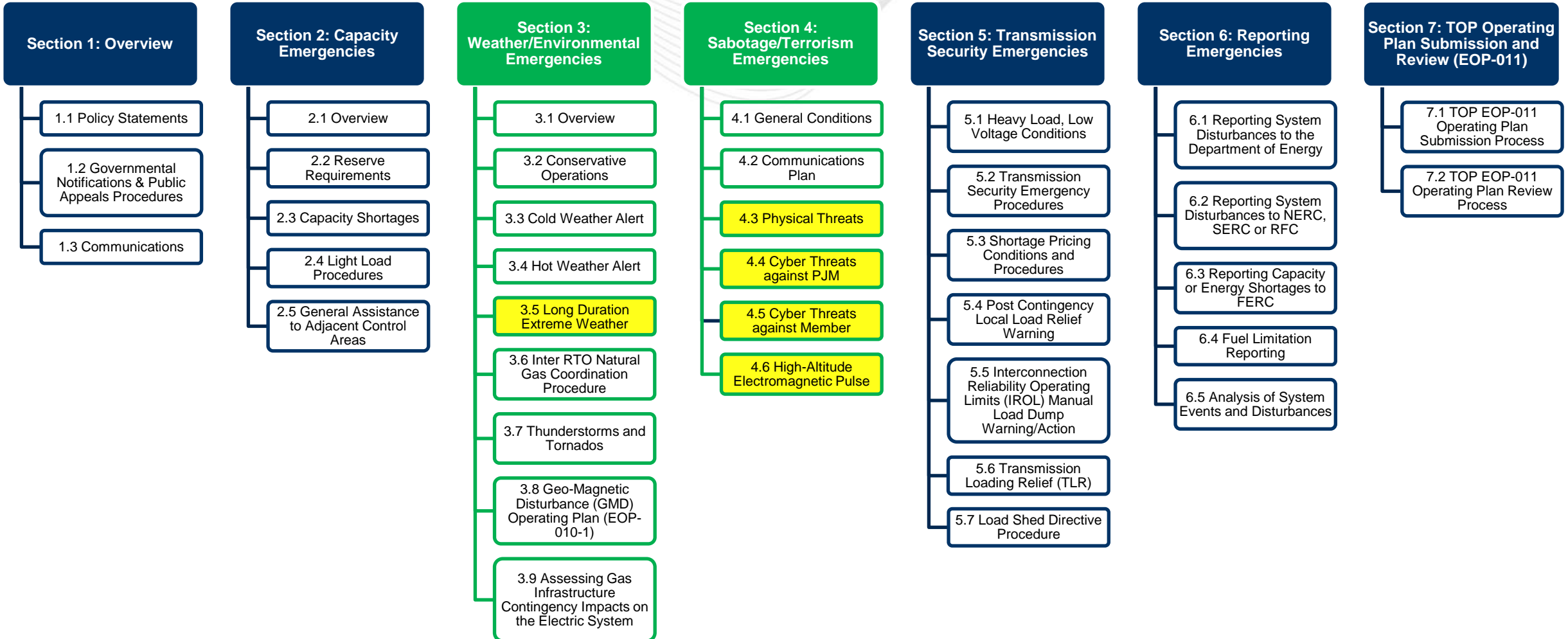
A Production System Change Freeze is a procedure that is implemented to ensure a stable production environment over a defined period of time.

The production change freeze has two objectives. First, it is designed to ensure staff is available for critical activities, should the need arise. Second, it is designed to help ensure a stable technical environment to support PJM's business and reliability functions.

The change freeze announcement will identify start date/time and the predicted duration or end date/time of the freeze period. At any point during the change freeze window, system conditions will be evaluated and an announcement regarding the lifting or extension of the change freeze will be made.

- Section 3.6 added language for disabling auto-reclose

- Transmission dispatchers place reclosers in service.
 - o Transmission dispatchers may elect to manually disable recloser on certain lines that experience multiple re-close attempts during storms or other times during increased likelihood of “non-self-clearing” faults.
 - o Transmission dispatchers may disable auto-reclose at their own discretion. However, Transmission dispatchers are required to inform PJM when they disable auto-reclose on any transmission facilities.



- New Section 3.5 added for “Long Duration Extreme Weather”

3.5 Long Duration Extreme Weather

To prepare for and operate through Extreme Weather events expected to last more than 72 hours, during which wide-scale fuel disruptions are expected, PJM may extend the “Resource Limited Unit” reporting requirement for generators to evaluate a timeframe beyond 72 hours, as needed. PJM may also change the minimum run time requirements for Fuel Limited Resources to be placed into the Maximum Emergency Category. Examples of long-duration Extreme Weather with the potential to cause wide-scale fuel disruptions include, but are not limited to:

- Extended Cold Weather
- Long-Duration Blizzard and/or Icing Conditions
- Wide-Area Flooding
- Impacts of Extreme Weather (i.e Hurricane Damage) expected to last more than 72 hours

As the Extreme Weather event progresses, PJM dispatchers will continuously evaluate the weather conditions, assess system damage, and gauge the severity of fuel disruption. As conditions change, PJM will update “Resource Limited Unit” reporting time-frame and minimum run time requirements for units in the Maximum Emergency Category. For Fuel Limitation Reporting requirements please refer to Section 6.4 of this manual.

- Section 6.4 added language to adjust “Resource Limited Unit” reporting time-frame and minimum run time requirements to place additional Fuel Limited Resources into the Maximum Emergency Category during long duration extreme weather events. Aligns with new section 3.5 requirements
 - For long-duration extreme weather conditions expected to cause wide-scale fuel disruptions, as outlined in Section 3.5, PJM may adjust “Resource Limited Unit” reporting time-frame and minimum run time requirements to place additional Fuel Limited Resources into the Maximum Emergency Category.

Section 4: Sabotage/Terrorism Emergencies

Physical Attacks Vs Cyber Attacks

PJM Manual 13: Emergency Operations
Section 4: Sabotage/Terrorism Emergencies

- Terrorist threats and/or attacks upon the transmission system and related infrastructures (i.e., Telecom, Fuel, Transportation)
- Intelligence from the Federal Government or other credible sources (i.e., DOE, DHS, Reliability Authority, PJM Member)
- Suspicious events on either PJM or neighboring systems
- Other system conditions or outages with unknown causes

The significant triggers for PJM action during crisis will be the Homeland Security Threat Levels and Threat Advisories. However, if PJM becomes aware of a possible threat before any one of these triggers (e.g., PJM sees a significant terrorist attack on CNS) PJM may decide to act before any such alerts. Each of these alert is further explained in the attached appendices.

PJM Actions
This section of the manual will address possible PJM conservative operations in the event of a man-made threat to the bulk power grid and/or other significant infrastructures. The tailored response to any of these triggers will include a multi-faceted plan to safeguard personnel and maintain reliable operations. The facets of this response include power system operations, communications, cyber security, and physical security. The emphasis of this section is upon the Operations and Communications measures that may be taken based upon the threat and intelligence.

As PJM progresses into ever increasing alert levels the actions of the higher level include the actions of the lower levels such that when the highest alert level is issued, PJM may have implemented all actions for prior threat levels. Given the ability for the Department of Homeland Security (DHS) to issue alerts out of sequence, the order that the steps are presented does not mandate a set implementation plan.

The DHS has revised the threat level system in order to simplify the threat notification process. The new system which is referred to as the National Terrorism Advisory System (NTAS) consists of the following two alerts:

- **Imminent Threat Alert:** warns of a credible, specific, and impending terrorist threat against the United States.
- **Elevated Threat Alert:** warns of a credible terrorist threat against the United States.

NTAS alerts also include a sunset provision which provides a specific end date for each alert while also allowing for extensions when new information or threats occur.

NTAS and other alerts and potential PJM and Member actions include:

NTAS Alert: No Alert Issued	
Operations	
No NTAS Alert Issued	Conditions Normal – Routine Operations and Communications

Additional Threat Alert Sources

Additional Threat Alert Sources	Actions
Cyber event has shut down control center EMS capability, OR physical attack at multiple sites (control center or grid assets-lines, substations, generators).	1. Operate to more conservative modeling measures which may include double contingencies, maximum credible disturbances, or lower reactive transfer limits 2. Increase Available Operating Reserve 3. Cancel selected Maintenance Outages – attempt to return selected outaged equipment to service. [Consider invoking a “no touch” maintenance stance] 4. Consider staffing selected substations for communications
Intelligence of an impending attack on a PJM facility.	5. Consider staffing critical combustion turbine sites (Seek TO’s recommendations)
Cyber event has shut down control center EMS capability, OR physical attack at multiple sites (control center or grid assets-lines, substations, generators).	6. Increase Synchronized Reserve 7. Obtain emergency energy bids as a precaution
Significant terrorist activity beyond the East Coast (situational dependent)	8. Initiate Black Start Assessment (SSR) to determine fuel limitations 9. Consider staffing Critical Black Start Units 10. PJM recommends enhanced physical security at critical substations

Revision: 65, Effective Date: 01/01/2018 PJM © 2018 71

PJM Manual 13: Emergency Operations
Section 4: Sabotage/Terrorism Emergencies

Operations

1. Reminders to all operators for increased Vigilance
2. PJM Operations Management review and discuss this section of the emergency operations manual
3. Increased Vigilance and Reporting

Communications

4. PJM passes along credible/actionable intelligence
5. All operations centers should review reporting requirements/process

NTAS Alert: ELEVATED THREAT LEVEL

Actions

Operations

1. Maintenance Outages Analyzed – additional coordination with TO/GO to confirm emergency return times, if necessary
2. Maximum Credible Contingencies analyzed by PJM Reliability Engineer
3. Increased Vigilance/Reporting
4. Analyze Hydro Schedules – for possible interruption to increase Black Start capability
5. Initiate Black Start Assessment (SSR) – to determine fuel limitations

Communications

6. Communicate threat over ALL-CALL
7. Satellite Phone Checks (daily upon initiation and weekly thereafter)
8. Enhance Voice Communications Security (Operators who do not recognize another operator, should call back to the entity or organizations should have a password to validate directives)
9. Enhance Cyber Security Scanning

Revision: 65, Effective Date: 01/01/2018 PJM © 2018 72

PJM Manual 13: Emergency Operations
Section 4: Sabotage/Terrorism Emergencies

Operations

1. Operate to more conservative modeling measures which may include double contingencies, maximum credible disturbances, or lower reactive transfer limits
2. Increase Available Operating Reserve
3. Cancel selected Maintenance Outages – attempt to return selected outaged equipment to service. [Consider invoking a “no touch” maintenance stance]
4. Consider staffing selected substations for communications
5. Consider staffing critical combustion turbine sites (Seek TO’s recommendations)
6. Increase Synchronized Reserve
7. Obtain emergency energy bids as a precaution
8. Initiate Black Start Assessment (SSR) to determine fuel limitations
9. Consider staffing Critical Black Start Units
10. PJM recommends enhanced physical security at critical substations

Communications

Revision: 65, Effective Date: 01/01/2018 PJM © 2018 73

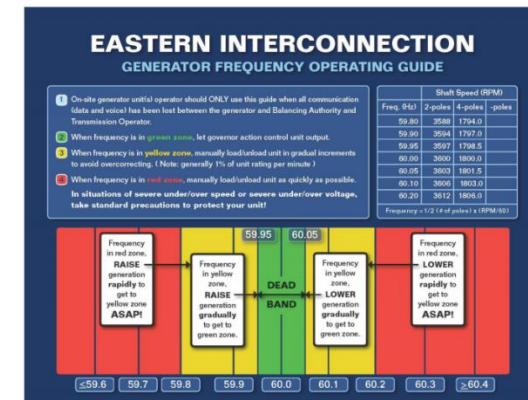
- Re-format – remove table and present actions in “PJM Actions” / “Member Actions” format to match rest of manual
- Subsection for Physical Attack
- Subsection for Cyber Attack against PJM
 - Loss of ICCP/EMS
 - Loss of internet
 - Loss of telecommunications
- New Subsection for Cyber Attack against member company (GO/TO)
- New Subsection for HEMP attack

- Section 4.1 deleted Exhibit 4 table
 - Former Exhibits 5 through 14 renumbered accordingly
 - Former Exhibit 4 content regarding “Elevated Threat Alert” reformatted in section 4.1 as a list of “PJM Actions” and “PJM Member Actions”
 - Former Exhibit 4 content regarding “Imminent Threat Alerts”, “Intelligence of an impending attack on a PJM facility”, “physical attack at multiple sites”, or “Significant terrorist activity beyond the East Coast” moved to section 4.3 as a list of “PJM Actions” and “PJM Member Actions”
 - Former Exhibit 4 content regarding “Cyber event has shut down control center EMS capability” moved to section 4.4 as a list of “PJM Actions” and “PJM Member Actions”
- New section 4.3 for PJM operational procedure for physical threats
 - Created from Former Exhibit 4 content regarding “Imminent Threat Alerts”, “Intelligence of an impending attack on a PJM facility”, “physical attack at multiple sites”, or “Significant terrorist activity beyond the East Coast” as a list of “PJM Actions” and “PJM Member Actions”
 - Updated “Operating Reserves” language to “30-Minute Reserves”
 - Added requirement for PJM to alert PJM’s Operations Emergency Response Team (OERT)

- New section 4.4 for PJM operational procedure for cyber threats against PJM
 - New section 4.4.1 for loss of ICCP or EMS capabilities operational procedure
 - Created from Former Exhibit 4 content regarding “Imminent Threat Alerts”, “Intelligence of an impending attack on a PJM facility”, “physical attack at multiple sites”, or “Significant terrorist activity beyond the East Coast” as a list of “PJM Actions” and “PJM Member Actions”
 - Updated “Operating Reserves” language to “30-Minute Reserves”
 - Added language to initiate “Manual Dispatch”
 - New section 4.4.2 for loss of internet operational procedure
 - New section 4.4.3 for loss of all telecommunications operational procedure
- New section 4.5 for PJM operational procedure for cyber threats against member company
- New section 4.6 for PJM operational procedure for High-Altitude Electromagnetic Pulse

- PJM performs constant cyber security monitoring. If the Security Monitoring Team determines there is a credible cyber threat that could impact operations:
 - PJM Incident Response Team (IRT) will meet to determine which systems are impacted.
 - IRT will contact Dispatch Shift Supervisor with impacts to operations.
 - Conservative Operations will be triggered by PJM Shift Supervisor as necessary.
 - PJM will notify members of impacted systems and necessary actions via the All-Call.

- For telecommunications disruptions, PJM will alert Incident Response Team (IRT) to begin internal recovery process. Additional actions will be as follows:
 - Loss of ICCP/EMS capabilities
 - Direct PJM dispatchers and Members to begin Manual Dispatch: directions in Manual 1, section 3.8.2
 - Additional PJM dispatchers and/or support staff may be required
 - Loss of Internet
 - Loss of Internet plans require TOs and GOs to call in with manual updates for internet based applications
 - Additional PJM dispatchers and/or support staff may be required
 - PJM has multiple levels of redundancy for verbal communication
 - Loss of all telecommunications
 - PJM will constantly attempt to establish communication to Transmission Owners and Generation Owners via all means of verbal communication
 - Reliability Guideline: [Generating Unit Operations During Complete Loss of Communications v2.0](#)



- Consistent Bad data or “Altered” data
 - Put company in ‘View Mode’ until data quality can be restored
 - Alert PJM Incident Response Team (IRT) to work with TO to resolve problem
- If a TO has an asset operated remotely by an unauthorized entity:
 - Alert Operations Emergency Response Team to determine best operational strategy
 - PJM shift supervisors will initiate Conservative Operations as necessary.
 - Call SOS-T conference to alert other Transmission Owners
 - Alert PJM IRT
 - Post to RCIS
 - Send All-Call
- Affected member company will verify protective relay settings of tariff facilities