



# Resiliency Update: Proposed M-13 Changes

Mr. Dean Manno  
PJM Interconnection

## **This is NOT a first read**

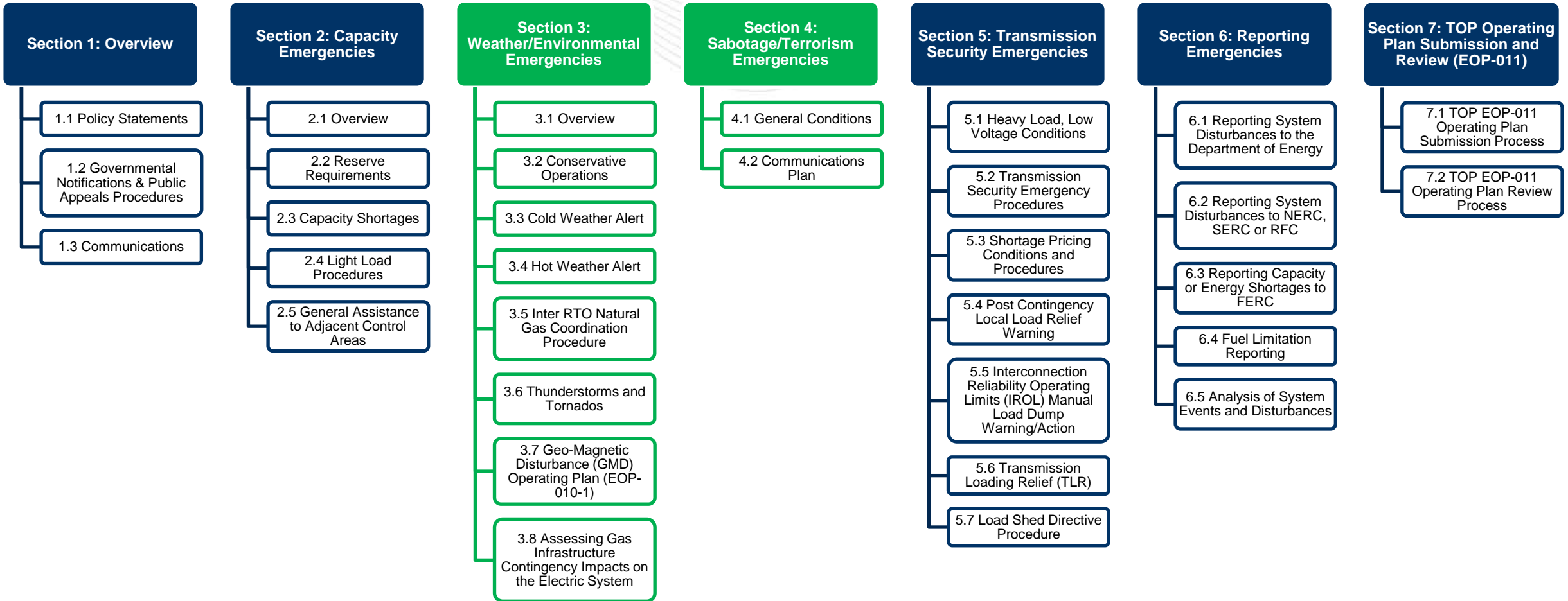
Purpose of this presentation is to review changes proposed by the SOS-T before drafting manual language

# Restructure Sections



# PJM Manual 13: Emergency Operations

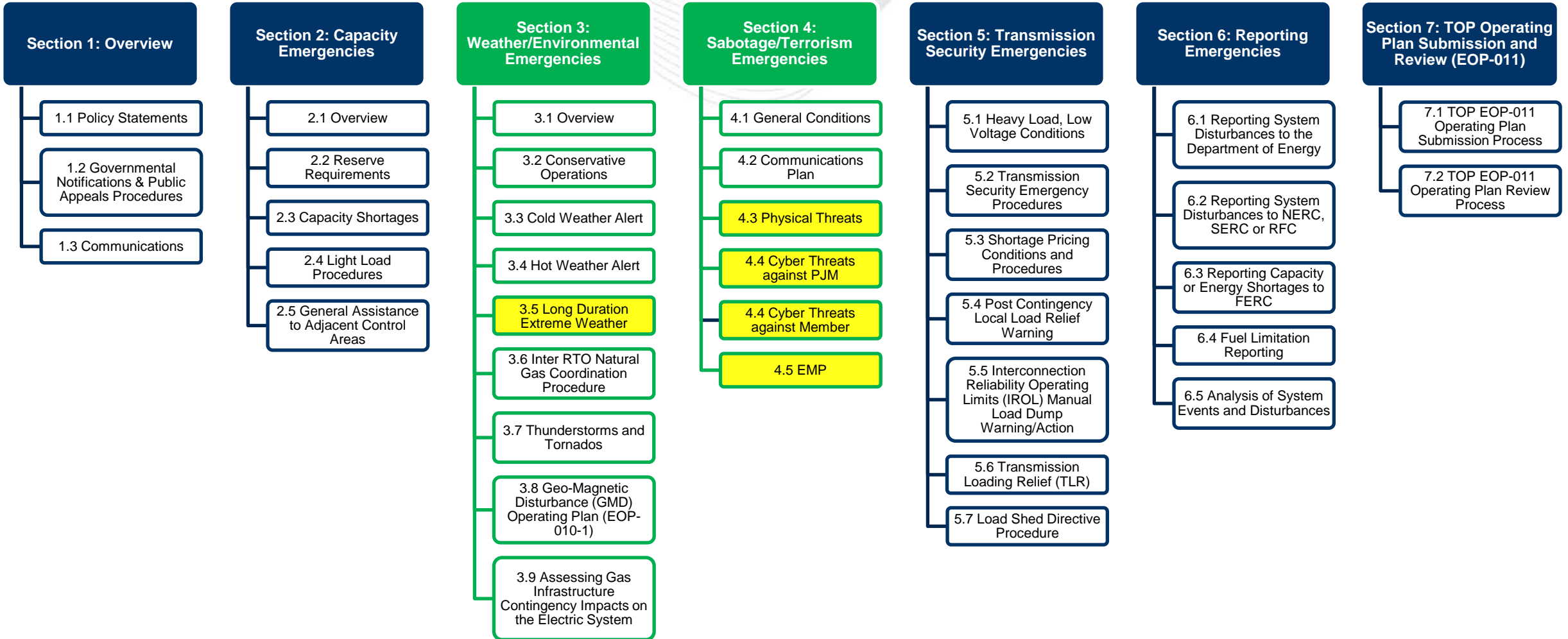
## Current Structure





# PJM Manual 13: Emergency Operations

## Current Structure



# New Controlling Actions

- During conservative operations, a Production System Change Freeze will be in effect: 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

*“The production change freeze is a procedure that is implemented to ensure a stable production environment over a defined period of time. A production change freeze is declared if PJM management decides conditions warrant it. Typical reasons for declaring a change freeze include extreme weather, system conditions, business continuity events, or staff availability.*

*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.”*

- **Clarify increase in “Operating Reserves” as “30 Minute Reserves”**
  - Adjustments generally consistent with those made in Day-Ahead
  
- **For Extreme Weather expected to last more than 72 hours, where wide-scale fuel disruptions are expected:**
  - (Extended cold-weather or blizzard conditions.)*
  - (Impacts of extreme weather (i.e. Hurricane damage) expected to last more than 3 days.)*
  - (Other weather conditions expected to cause extended wide-scale fuel disruptions)*
  - **Extend “Resource Limited Unit” reporting for generators to evaluate a time frame beyond 72 hours, as needed.**
  - **Report any other constraints that will restrict generator run times.**



- Some companies may elect to manually disable Auto-Reclose Relays on certain lines that experience multiple re-close attempts during storms or other times during increased likelihood of “non-self-clearing” faults. TO’s may disable auto-reclose at their own discretion. However, Transmission Owners are required to inform PJM when they disable auto-reclose on any transmission facilities.



# Section 4: Sabotage/Terrorism Emergencies

## Physical Attacks Vs Cyber Attacks

pjm 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 those triggers (e.g., PJM sees a significant terrorist attack on CNN) PJM may decide to act before any such alerts. Each of these alerts 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	Actions
No NTAS Alert Issued	Conditions Normal - Routine Operations and Communications

Additional Threat Alert Sources

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

pjm 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
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

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
Intelligence of an impending attack on a PJM facility.	2. Increase Available Operating Reserve
Cyber event has shut down control center EMS capability, OR physical attack at multiple sites (control center or grid assets-lines, substations, generators).	3. Cancel selected Maintenance Outages – attempt to return selected outaged equipment to service. [Consider invoking a "no touch" maintenance stance]
Significant terrorist activity beyond the East Coast (situational dependent)	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.

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
  - Unchanged
- Breakout 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 EMP attack

- Manual Dispatch Instructions
- Verbal Communication Protocols
- Company View Mode
- PJM Operations Emergency Response Team (OERT) Actions
- PJM Incident Response Team (IRT) Actions
- SOS-T Conferences
- RCIS Reporting
- All-Call Alerts
- NERC Reliability Guideline: Generating Unit Operations During Complete Loss of Communications