8. If a non-routine shutdown occurred, refer Generator to follow the facility's trip investigation procedure
9. Save Outage / Derate Request Form on SharePoint.
10. Refer to the new Real-Time Monitoring & Dispatching Process Document for information on reallocating AS that the Resource can no longer provide.

3.1.2. Generator Forced Outage Completion or Extension (Generator)

Procedural Steps

1. On or about the preceding day of the planned outage end time, the generating facility shall confirm impending completion of the outage via telephone call to GenDesk and Austin Energy (for FPP 1 & 2)
2. Update Outage / Derate Request Form as needed to reflect changes greater than 2 hours. Send to "GenDesk Outage" email group.
3. Upon completion of outage finalize and archive Outage / Derate Request Form. Send to "GenDesk Outage" email group.

3.1.3. Generator Forced Outage Completion or Extension (GenDesk)

Procedural Steps

1. Generator declares forced outage is completed or there is need for extension of outage
2. Generator forced outage completion or extension is communicated / scheduled with ERCOT
   a. GenDesk enters outage completion time or extension in PCI Outage Scheduler, submit to ERCOT and startup included in Current Operating Plan if appropriate
   b. Include Austin Energy in discussion for FPP 1 & 2
   c. GenDesk to discuss with generating facility as necessary

3.2. Opportunity Outages

3.2.1. Forced Outage occurs prior to Planned Outage (Generator)

Failure of (or necessary repairs to) critical power plant equipment occurs that triggers a forced outage within 8 days of previously scheduled and approved Planned Outage.

Procedural Steps

1. Inform GenDesk and Austin Energy (for FPP 1 & 2) of Forced Outage
2. Ensure safe and orderly shutdown
3. The resource may remain off-line and start the approved planned outage earlier than scheduled
4. Submit Outage / Derate Request Form to GenDesk as soon as details of event are available Send to "GenDesk Outage" email group
5. Follow the facility's trip investigation procedure

3.2.2. Forced Outage occurs prior to Planned Outage (GenDesk)

When a specific resource has been forced off-line due to a Forced Outage and the resource has been previously approved for a Planned Outage to start within the next 8 days, ERCOT may approve the resource to remain off-line and start the Planned Outage earlier than scheduled.

Procedural Steps

1. Call facility (as soon as practicable), requesting information for cause of trip and expected return to service time
2. Notify ERCOT as soon as practicable
3. Verify in ERCOT Outage scheduler the Planned Outage start date is 8 days of less of current Forced Outage

4. If the Forced Outage is on FPP 1 & 2 contact Austin Energy and discuss options to start Planned Outage earlier than scheduled
5. Coordinate with the resource facility (Austin Energy for FPP 1 & 2) to determine whether contractors are able to start planned outage earlier than scheduled
6. Coordinate with the Day-Ahead group to determine the financial exposure to start planned outage earlier than scheduled
7. Build a Forced Outage in PCI Outage Scheduler and submit to ERCOT MIS Outage Scheduler during the Adjustment Period.

***NOTE* The Forced Outage end date and time cannot overlap with the approved Planned Outage planned start date, time.**

8. Once submitted to ERCOT, a warning message "Conditions for a resource Opportunity Outage are met, etc." in the ERCOT Outage scheduler
9. The ERCOT Outage scheduler will display "Take Opportunity" selection, select yes (Appendix E)
10. Once approved by ERCOT, this Opportunity Outage basically fills in the time period between the Forced Outage and the Planned Outage

3.3. Outage of Transmission Equipment Owned by Generator

Transmission equipment that is owned by the generation facility may need to be removed from service for repair or replacement while resource stays on-line. Normally these outages are entered into the outage scheduler by the Transmission owner however there may be occurences when the GenDesk must enter these outages. Follow the steps in Appendix G to enter transmission equipment outages in the ERCOT outage scheduler.

3.3.1. Request Outage of Transmission Equipment (Generator)

Procedural Steps

1. Generating facility coordinates and schedules work with LCRATSP (SOCC)
2. Notify GenDesk of outage request by telephone call
3. If the reason for the outage is non-routine due to equipment failure or possible misoperation and operation of the resource will result in a single contingency, or will otherwise reduce system reliability, notify Engineering to review.
4. Engineer reviews situation and prepares report for submittal to GenDesk
5. Send report to GenDesk
6. Save report in EDMS

3.3.2. Coordinate Outage of Transmission Equipment (GenDesk)

Procedural Steps

1. Receive outage request from Resource Facility
2. Verify outage with interconnecting Transmission Owner and monitor / ensure Transmission Owner coordinates outage with ERCOT
3. GenDesk decides whether to submit the Engineer's report (if report was created) to ERCOT

3.4. Outage of Telemetry / Control / Communication Equipment

3.4.1. Emergency Outage of Telemetry / Control / Communication Equipment (GenDesk)

Procedural Steps

1. Call ERCOT and other affected parties to inform them of the outage
2. Provide estimate of duration
3. Complete work to restore service

4. Inform all affected parties of equipment back in service

3.4.2. Planned Outage of Telemetry / Control / Communication Equipment (GenDesk)

Procedural Steps

1. Identify need for outage
2. Determine scope and necessary duration
3. Determine desired start date / time
4. GenDesk and affected party discuss the outage request
   a. Include ERCOT in discussion if outage impacts data and communication exchange with this entity
   b. Include Austin Energy in discussion for FPP 1 & 2
   c. GenDesk to discuss with generating facility as necessary
5. Negotiate / agree on outage start date / time and duration – E-Mail confirmation
6. Plan and execute outage as agreed
7. Inform all affected parties of equipment back in service

4 Withdrawal of Approval for Planned Outages of Resource from ERCOT

4.1. ERCOT Issues an Advance Action Notice (AAN)

1. If ERCOT believes it cannot maintain reliability and has exercised all other means to resolve and the cancellation or early return to service of a resource that has been approved for an outage, then they may issue an Advance Action Notice.
2. The AAN must state the date and time the possible Emergency Condition would begin as well as the date and time it would end. ERCOT must also state what actions they might take including the capacity amounts they would seek from an Outage Adjustment Evaluation (OAE).
3. ERCOT must issue and AAN at least 24 hours before it conducts and OAE and ERCOT should not issue an Outage Schedule Adjustment (OSA) unless an OAE has been concluded.
4. Once ERCOT issues an AAN, the GenDesk will notify the GenDesk Manger and inform him ERCOT will be conducting an OAE.
5. Gendesk will identify any planned outages that might be affected during the dates and times specified in the AAN.
6. If any planned outages are able to be rescheduled before ERCOT conducts the OAE, GenDesk should contact ERCOT and inform them of which outages will be changed and update said outages in the ERCOT Outage Scheduler utilizing PCI.
7. If any outages are cancelled or rescheduled, update GenDesk will update the COP and submit to ERCOT.
8. Update logbook accordingly.

4.2. ERCOT Issues Outage Schedule Adjustment (OSA)

1. ERCOT notifies GenDesk that it has issued an OSA for an LCRA resource.
2. GenDesk will notify GenDesk manager of OSA and which resource is affected.
3. The decision to leave the resource online or place the resource in an OFF status will be determined and the GenDesk will be notified.
4. If the unit remains online, the resource status must be updated to “ONRUC”.
    a. Any resource that remains online and uses an “ONRUC” status must remain at LSL until dispatched by SCED above that level.
    b. The EOC for the resource must also be updated to the System Wide Cap (SWC).
5. If the resource is shown in an “OFF” status, then the resource must remain off-line and cannot be self-committed during the hours of the OSA. The resource will be available for the RUC process.
6. Any outage affected by an OSA may be rescheduled as long as the new outage does not start before the OSA ends.

5 Forms and Resource Specific Procedures

5.1. Outage / Derate Request Form

The Outage / Derate Request Form can be found in the 'Forms Library' on SharePoint using the following link:

http://team.lcra.org/sites/GOP_Compliance/Outage Derate Forms/Forms/AllItems.aspx

6. Document Control

Prepared by:
KEMA Inc 7/18/2007

6.1. Review Log

Reviewed By	Title	Date
Facility NERC Coordinators, Greg Graham, Tony Rossi, Jim Guenther	SME Team	07/07/2009
Facility NERC Coordinators, Jay Watson, Tony Rossi, Jim Guenther, Arnold Lewis	SME Team	04/13/2010
Jay Watson, Greg Pyka	SME Team	05/25/2011
Facility NERC Coordinators, Jay Watson, Arnold Lewis	SME Team	08/05/2011
Jay Watson, Greg Pyka	SME Team	10/25/2011
Jay Watson, Greg Pyka	SME Team	03/13/2012
Note Jay Watson, Greg Pyka	SME	10/3/2012
Jay Watson, Greg Pyka, Alton Matthews, Clifton Dukes	SME	8/16/2013 & 9/27/2013
Mike Hale, Greg Pyka	SMEs	02/12/2015
Greg Pyka, Darren Hughes	SME	08/31/2016
Greg Pyka Ron Friday	SME	1/6/2020 4/16/2020 & 12/9/2020
Ron Friday	SME	11/3/2021

6.2. Change History

The change history below reflects changes to the Manual or its structure.

Version	Description of change	Date
01.00	Initial issue	7/18/2007
02.00	General revisions to incorporate AESI recommendations and updates	11/25/2008

Version	Description of change	Date
03.00	Performed annual review 2.1.1 Clarified frequencies for reviews 2.1.2 Added section for GenDesk long-term planning coordinator steps 2.1.3 Added note to step 3 2.1.4 Changed Pmax to Seasonal HSL 2.3.1 Clarified timeframe for confirmation with GenDesk 2.3.3 Clarified timeframes and elaborated use of Outage / Derate Request form 2.4.1 step 12 Changed procedure reference from "86 lockout" to "trip investigation" 3 Deleted outage guidelines 3.1 Clarified long-term / short-term responsibilities 3.2 Modified Outage / Derate Request form 4.1 Changed review period to calendar year 4.3 Added section for approval signatures Deleted compliance monitoring section	08/17/2009
04.00	Performed annual review 1.2 Changed reference from VAR-002 to IRO-004; also changed ERCOT reference to Nodal Protocol 3.1 1.3 Updated flowchart Section 2 general changes: Changed "resource plan" to "current operating plan". Clarified locations for documentation storage. Clarified when to use the "Outage / Derate Request Form". 2.1.1 Clarified that long term outage plans are maintained in spreadsheet format by GenDesk Long Term Outage Coordinator and the "Outage / Derate Request Form" is not used for long term outage planning. 2.1.3 Changed timeframe for near-term outages from 14 days to 30 days. 2.1.4 Removed criteria for reporting derates – LCRA practice is to report all derates 2.4.1 Clarified when engineering review is required when generator-owned transmission equipment is removed from service 2.6 Deleted unnecessary procedures related to external requests for outages. 3.1 Personnel names replaced with job titles 3.2 Updated form Appendix F Updated contact list for ERCOT Outage Coordination team	04/19/2010

Version	Description of change	Date
04.01	Performed periodic review. Updated to reflect changes due to implementation of Nodal Market. Changed references from Texas Market Link to ERCOT Market Information System (MIS). Updated steps involved with entering outage information in PCI. Changed criteria for derates to match new ERCOT definition. Deleted cyclic review process. Updated Outage / Derate Request Form. Updated screen shots in Exhibit E for PCI and MIS.	8/05/2011
04.02	Performed periodic review. Updated to reflect changes due to changes in the Nodal Market.	08/25/2011
04.03	1.2 Updated Related Documents section 2.1.4 Revised to include 15 minute notification of Derate 2.1.4 (8) Referenced to Real-Time Resource Monitoring & Dispatching Process Document 2.3.2 Revised to include 15 minute notification of Forced Outage 2.3.2 (12) Referenced to Real-Time Resource Monitoring & Dispatching Process Document Description of Change field – Included new Appendix F (Combined Cycle Outage Scheduling in PCI). Appendix G is not listed in the table of contents. Quick link from table of contents section does not relocate you to the Appendix F. Appendix F, page 37, first sentence, uild should be “Build.”	03/13/2012
04.04	Revised procedure to handle derating of a resource 2.1.2 Removed long term planning coordinator 2.1.3 Removed derate reference, defined planned and maintenance outage 2.1.4 Removed derate reference 2.3 Added new section for derate 2.3.2 Defined the 48 hour duration of a derate 2.4.2 Removed derate reference 2.5 Added Opportunity Outage section Removed section 3 – Process Flow Diagram Added Appendix-G	10/3/2012

Version	Description of change	Date
05.00	Major Revision 2.1.2 Updated location of long term outage schedule 2.3.2 Updated new ERCOT Protocol requirements pertaining to derates 2.3.2.1 New section devoted to derates lasting longer 48 hours 2.3.2.2 New section devoted to derates less than 48 hours and modified all procedural steps 3.1.2 Realigned the procedural steps and included notification to GenDesk Mgr in the event of a 1000mw loss of generation 4.2 Updated the outage/derate form Appendix F, updated to include other scenarios Appendix I, new user guide added	09/27/2013
05.01	1.2 Updated Related Documents section 2.1.3 Clarified the language regarding 45 day outage submittal 2.1.4 (2) Removed requirement to notify ERCOT via phone call 2.2.4 Added step 3, shall notify ERCOT prior to resuming service 2.3.2.1 Removed 15 minute notification to ERCOT of derate 2.3.2.2 Removed 15 minute notification to ERCOT of derate 3.1.1 Removed 15 minute notification to ERCOT of derate	02/12/2015
05.02	1.2 Updated Related Documents section 2.1.2 (2) Clarified the GenDesk manager will track long term outages 2.2.2 (1) Removed reference to resource plan and inserted COP 2.2.4 (3) Clarified document storage area 3.1.2 (7) Updated to reflect NERC Event Reporting Form 4.1 Removed section Appendices have been updated as follows: **Appendix A – now ERCOT Protocols – Outage Information** (consolidated Appendix A-D into one appendix) **Appendix B – now ERCOT Outage Scheduler System** (previously Appendix E) **Appendix C – now Combined Cycle Outage Scheduling in PCI** (previously Appendix F) **Appendix D – now ERCOT Outage Coordination Organization** (previously Appendix G) Appendix E – prior contents of this appendix was removed entirely; **Appendix E is now ERCOT Outage Scheduler – Opportunity Outage** (previously Appendix H) **Appendix F – now Multiple Derates on a Single Resource** (previously Appendix I)	08/31/2016

Version	Description of change	Date
05.03	1.2 Updated Related Documents section 2.1.4 Added Planned Outage on Reliabiltiy Resource – Blackstart (Generator) 2.1.5 Added Maintenance Level II & III on Reliability Resource – Blackstart (Generator) 3.1.1 Added All Forced Reliability Resources, TSP/ERCOT notification	4/16/2020
05.04	1.2 – Related Documents – updated to include ERCOT Protocol 3.1.6.9 *Withdrawal of Approval or Acceptance and Rescheduling of Approved or Accepted Planned Outages of Resource Facilities* 2.1.7 – Removed section 2.1.7 titled Outage Issues Identified (GenDesk) NEW section 4. - Withdrawal of Approval for Planned Outages of Resource from ERCOT	11/3/2021

6.3. Approval

	Major Revision	Management Approval Required
X	Minor Revision	Management Approval Not Required

Outage Scheduling Process / Version 05.04

Authorized by:

Joel Firesetone, VP, Regulatory and Market Compliance
(Authorization made via MS Outlook voting feature. Please see attached report.)

Approval:

(Approval made via MS Outlook voting feature. Please see attached report.)

Darren Hughes	Manager, GenDesk
Ron Friday	Real-Time Operations Coordinator

Teresa Krabe

From:	Teresa Krabe
Sent:	Wednesday, November 3, 2021 9:50 AM
To:	Joel Firestone; Darren Hughes; Ron Friday
Cc:	Teresa Krabe (Teresa.Krabe@lcra.org)
Subject:	URGENT - APPROVAL REQUEST: Outage Scheduling Process, V05.04
Attachments:	Outage Scheduling V05.04.docx

Tracking:

Recipient	Response
Joel Firestone	Yes, I have reviewed the document(s) and APPROVE of the contents: 11/12/2021 2:39 PM
Darren Hughes	Yes, I have reviewed the document(s) and APPROVE of the contents: 11/3/2021 7:13 PM
Ron Friday	Yes, I have reviewed the document(s) and APPROVE of the contents: 11/8/2021 6:38 AM
Teresa Krabe (Teresa.Krabe@lcra.org)	
Teresa Krabe	Yes, I have reviewed the document(s) and APPROVE of the contents: 11/3/2021 9:54 AM

An immediate review of the ***Outage Scheduling Process, V05.04*** was conducted which required revision. The document now requires your review/approval. A clean copy is attached. All changes can be found in the Change History table on page 17.

Please complete your review and submit your response - while on the LCRA network using your LCRA issued computer – by way of the vote feature located at the top of this email by **Friday, November 5, 2021**. The version effective date within the document header will be identified as the date the last approval is obtained and updated upon completion of the voting process.

Thank you,

Teresa Krabe
Lower Colorado River Authority | Regulatory and Market Compliance Analyst, Sr.
O 512-578-4040 C 512-483-1825
Teresa.Krabe@LCRA.org

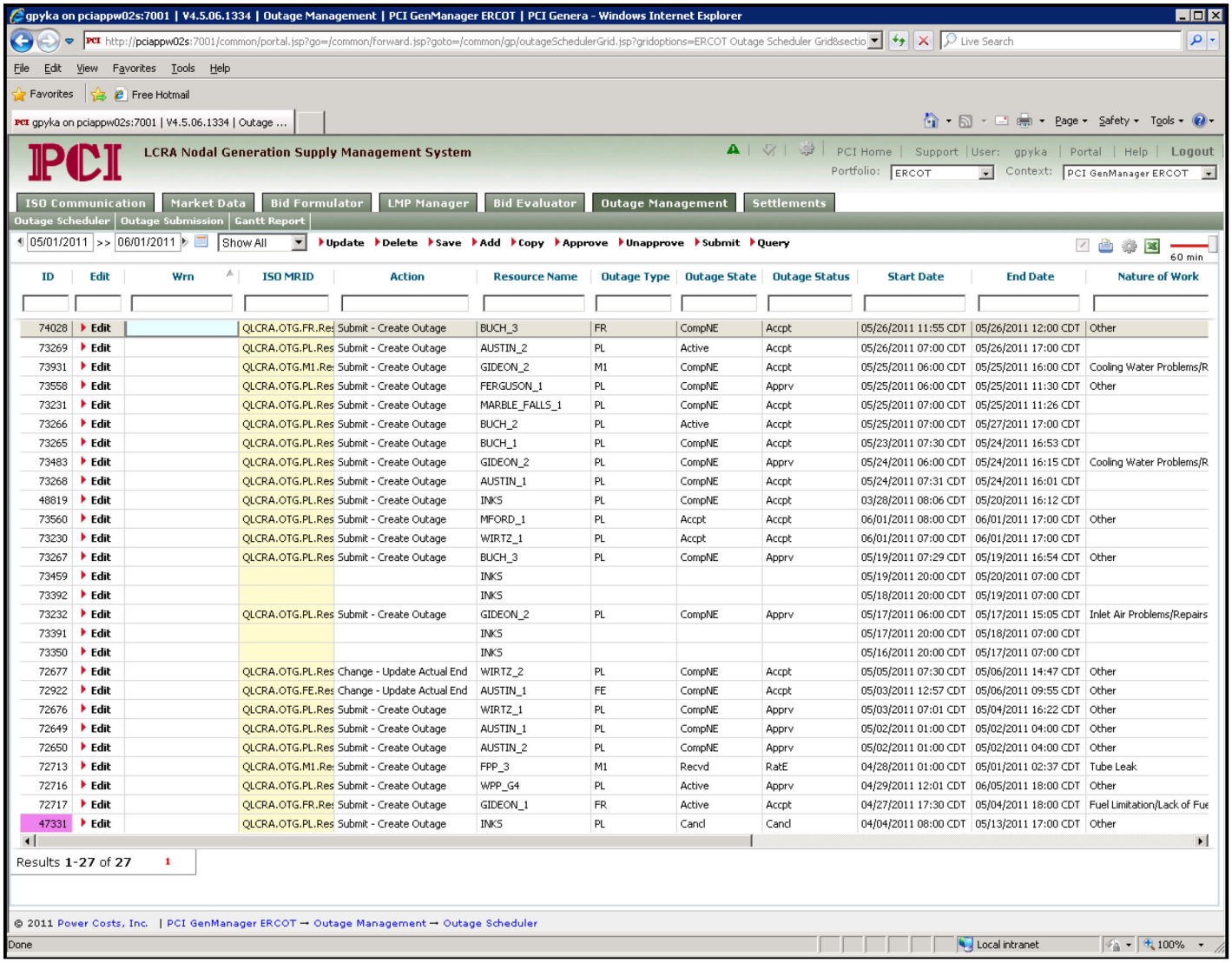
Enhancing the Lives of Texans

1

7. Appendix A – ERCOT Outage Scheduler System

PCI Outage Scheduler

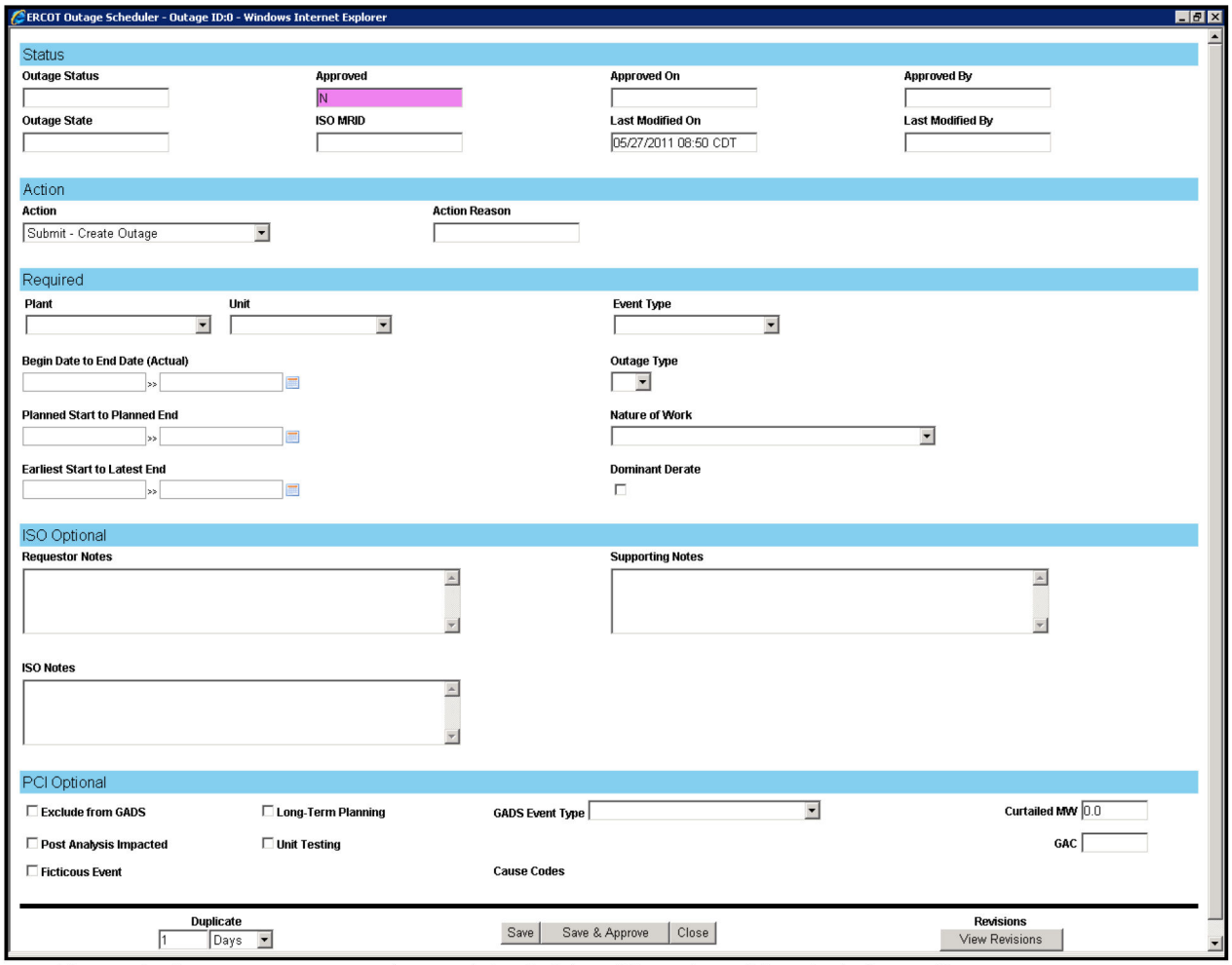
If a Resource trips off-line, first, notify ERCOT verbally per our normal procedures. Using PCI Outage Scheduler, submit the outage as described below.



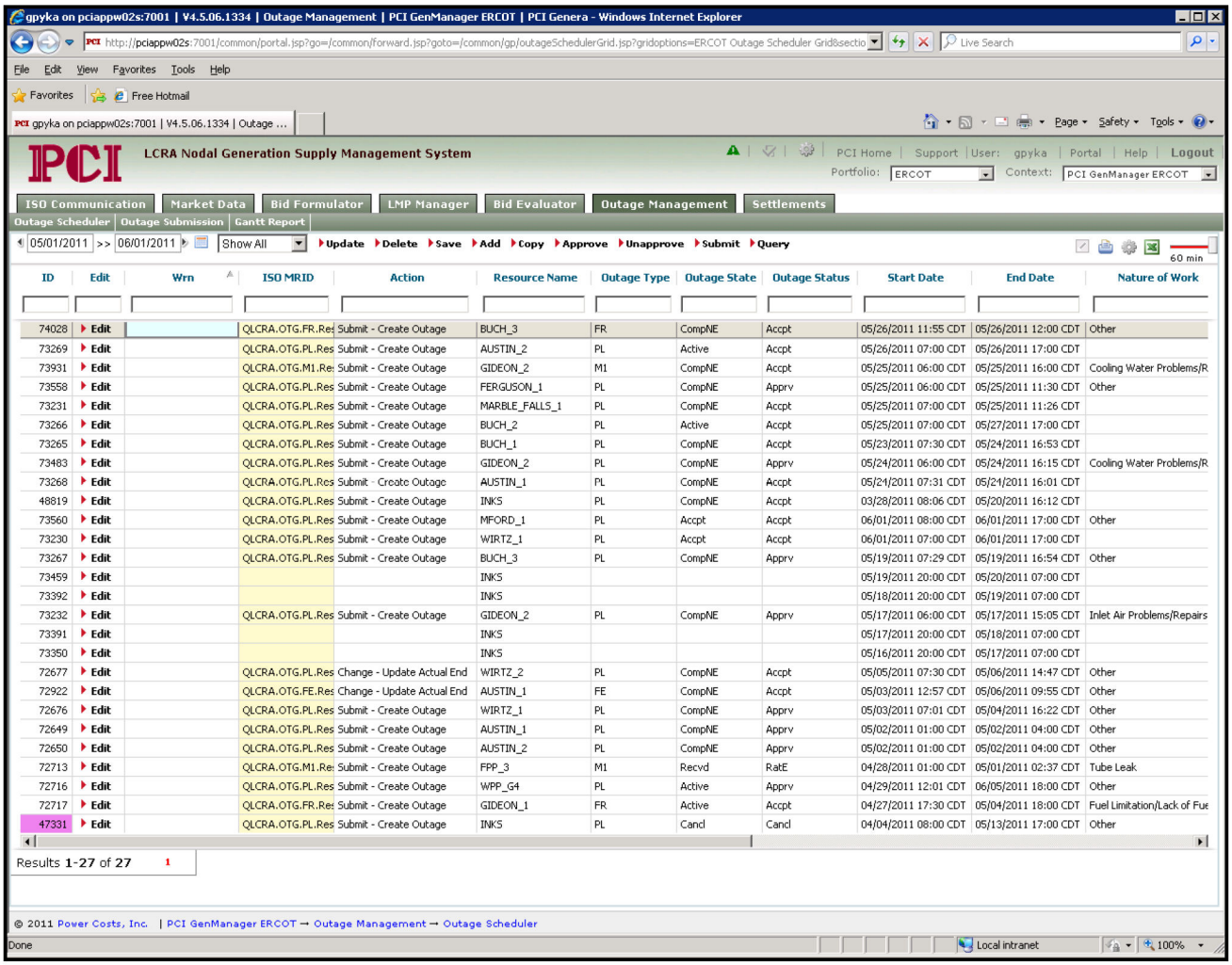
ID	Edit	Wrn	ISO MRID	Action	Resource Name	Outage Type	Outage State	Outage Status	Start Date	End Date	Nature of Work
74028	Edit		QLCRA.OTG.FR.Res	Submit - Create Outage	BUCH_3	FR	CompNE	Accpt	05/26/2011 11:55 CDT	05/26/2011 12:00 CDT	Other
73269	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	AUSTIN_2	PL	Active	Accpt	05/26/2011 07:00 CDT	05/26/2011 17:00 CDT	
73931	Edit		QLCRA.OTG.M1.Re	Submit - Create Outage	GIDEON_2	M1	CompNE	Accpt	05/25/2011 06:00 CDT	05/25/2011 16:00 CDT	Cooling Water Problems/R
73558	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	FERGUSON_1	PL	CompNE	Apprv	05/25/2011 06:00 CDT	05/25/2011 11:30 CDT	Other
73231	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	MARBLE_FALLS_1	PL	CompNE	Accpt	05/25/2011 07:00 CDT	05/25/2011 11:26 CDT	
73266	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	BUCH_2	PL	Active	Accpt	05/25/2011 07:00 CDT	05/27/2011 17:00 CDT	
73265	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	BUCH_1	PL	CompNE	Accpt	05/23/2011 07:30 CDT	05/24/2011 16:53 CDT	
73483	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	GIDEON_2	PL	CompNE	Apprv	05/24/2011 06:00 CDT	05/24/2011 16:15 CDT	Cooling Water Problems/R
73268	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	AUSTIN_1	PL	CompNE	Accpt	05/24/2011 07:31 CDT	05/24/2011 16:01 CDT	
48819	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	INKS	PL	CompNE	Accpt	03/28/2011 08:06 CDT	05/20/2011 16:12 CDT	
73560	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	MFORD_1	PL	Accpt	Accpt	06/01/2011 08:00 CDT	06/01/2011 17:00 CDT	Other
73230	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	WIRTZ_1	PL	Accpt	Accpt	06/01/2011 07:00 CDT	06/01/2011 17:00 CDT	
73267	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	BUCH_3	PL	CompNE	Apprv	05/19/2011 07:29 CDT	05/19/2011 16:54 CDT	Other
73459	Edit				INKS				05/19/2011 20:00 CDT	05/20/2011 07:00 CDT	
73392	Edit				INKS				05/18/2011 20:00 CDT	05/19/2011 07:00 CDT	
73232	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	GIDEON_2	PL	CompNE	Apprv	05/17/2011 06:00 CDT	05/17/2011 15:05 CDT	Inlet Air Problems/Repairs
73391	Edit				INKS				05/17/2011 20:00 CDT	05/18/2011 07:00 CDT	
73350	Edit				INKS				05/16/2011 20:00 CDT	05/17/2011 07:00 CDT	
72677	Edit		QLCRA.OTG.PL.Res	Change - Update Actual End	WIRTZ_2	PL	CompNE	Accpt	05/05/2011 07:30 CDT	05/06/2011 14:47 CDT	Other
72922	Edit		QLCRA.OTG.FE.Res	Change - Update Actual End	AUSTIN_1	FE	CompNE	Accpt	05/03/2011 12:57 CDT	05/06/2011 09:55 CDT	Other
72676	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	WIRTZ_1	PL	CompNE	Apprv	05/03/2011 07:01 CDT	05/04/2011 16:22 CDT	Other
72649	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	AUSTIN_1	PL	CompNE	Apprv	05/02/2011 01:00 CDT	05/02/2011 04:00 CDT	Other
72650	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	AUSTIN_2	PL	CompNE	Apprv	05/02/2011 01:00 CDT	05/02/2011 04:00 CDT	Other
72713	Edit		QLCRA.OTG.M1.Re	Submit - Create Outage	FPP_3	M1	Recvd	RatE	04/28/2011 01:00 CDT	05/01/2011 02:37 CDT	Tube Leak
72716	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	WPP_G4	PL	Active	Apprv	04/29/2011 12:01 CDT	06/05/2011 18:00 CDT	Other
72717	Edit		QLCRA.OTG.FR.Res	Submit - Create Outage	GIDEON_1	FR	Active	Accpt	04/27/2011 17:30 CDT	05/04/2011 18:00 CDT	Fuel Limitation/Lack of Fue
47331	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	INKS	PL	Cancl	Cancl	04/04/2011 08:00 CDT	05/13/2011 17:00 CDT	Other

PCI Outage Scheduler:

a. Content: select “PCI GenManager ERCOT”
b. Select “Outage Management”
c. Select “Outage Scheduler”
d. Select appropriate start/end date
e. Select “Update”
f. Select “Add” to enter a new outage/derate



a. New window opens up and populate fields with outage/derate information
b. "Action Field" – Select Submit-Create Outage for all outages/derates
c. "Plant" – Select appropriate Resource Facility
d. "Unit" – Select appropriate Resource
e. "Event Type" – Select EOO-PCI OS-Outage (never use CHCL-Outage Scheduler)
f. "Begin Date to End Date (Actual)" – Select appropriate time line for outage
g. "Outage Type"
    i. FE – Forced Extension
    ii. FR – Forced Outage or Forced Reduction (Derate)
    iii. M1 – Maintenance Level 1
    iv. M2 – Maintenance Level 2
    v. M3 – Maintenance Level 3
    vi. PL – Planned Outage
    vii. RS – Reliability Resources (RMR, Black Start Resources)
    viii. UE – Unavoidable Extension
h. "Nature of Work" – Select appropriate reason
i. "Requestor/Supporting Notes" – must populate fields when "other" was selected in "Nature of Work" field (providing more details to ERCOT of outage)
j. "Save & Approve" – Saves all data within PCI

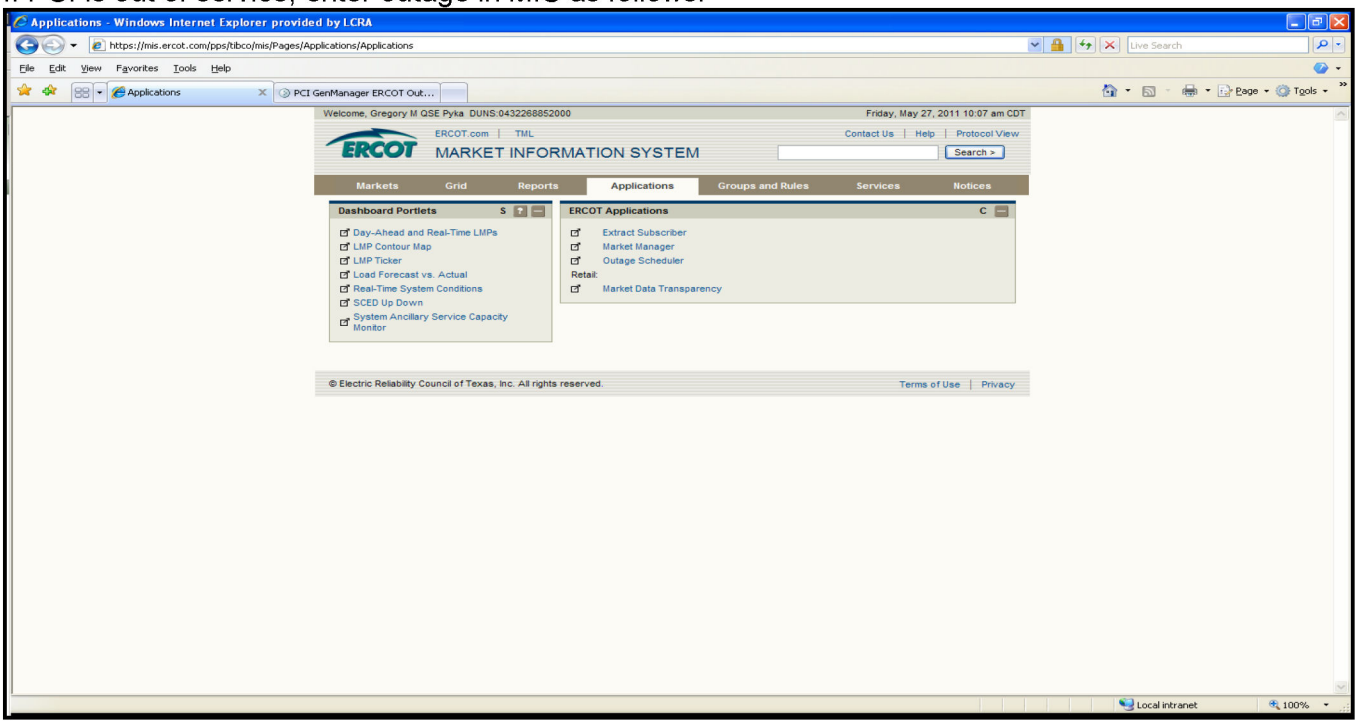


ID	Edit	Wrn	ISO MRID	Action	Resource Name	Outage Type	Outage State	Outage Status	Start Date	End Date	Nature of Work
74028	Edit		QLCRA.OTG.FR.Res	Submit - Create Outage	BUCH_3	FR	CompNE	Accpt	05/26/2011 11:55 CDT	05/26/2011 12:00 CDT	Other
73269	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	AUSTIN_2	PL	Active	Accpt	05/26/2011 07:00 CDT	05/26/2011 17:00 CDT	
73931	Edit		QLCRA.OTG.M1.Res	Submit - Create Outage	GIDEON_2	M1	CompNE	Accpt	05/25/2011 06:00 CDT	05/25/2011 16:00 CDT	Cooling Water Problems/R
73558	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	FERGUSON_1	PL	CompNE	Apprv	05/25/2011 06:00 CDT	05/25/2011 11:30 CDT	Other
73231	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	MARBLE_FALLS_1	PL	CompNE	Accpt	05/25/2011 07:00 CDT	05/25/2011 11:26 CDT	
73266	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	BUCH_2	PL	Active	Accpt	05/25/2011 07:00 CDT	05/27/2011 17:00 CDT	
73265	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	BUCH_1	PL	CompNE	Accpt	05/23/2011 07:30 CDT	05/24/2011 16:53 CDT	
73483	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	GIDEON_2	PL	CompNE	Apprv	05/24/2011 06:00 CDT	05/24/2011 16:15 CDT	Cooling Water Problems/R
73268	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	AUSTIN_1	PL	CompNE	Accpt	05/24/2011 07:31 CDT	05/24/2011 16:01 CDT	
48819	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	INKS	PL	CompNE	Accpt	03/28/2011 08:06 CDT	05/20/2011 16:12 CDT	
73560	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	MFORD_1	PL	Accpt	Accpt	06/01/2011 08:00 CDT	06/01/2011 17:00 CDT	Other
73230	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	WIRTZ_1	PL	Accpt	Accpt	06/01/2011 07:00 CDT	06/01/2011 17:00 CDT	
73267	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	BUCH_3	PL	CompNE	Apprv	05/19/2011 07:29 CDT	05/19/2011 16:54 CDT	Other
73459	Edit				INKS				05/19/2011 20:00 CDT	05/20/2011 07:00 CDT	
73392	Edit				INKS				05/18/2011 20:00 CDT	05/19/2011 07:00 CDT	
73232	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	GIDEON_2	PL	CompNE	Apprv	05/17/2011 06:00 CDT	05/17/2011 15:05 CDT	Inlet Air Problems/Repairs
73391	Edit				INKS				05/17/2011 20:00 CDT	05/18/2011 07:00 CDT	
73350	Edit				INKS				05/16/2011 20:00 CDT	05/17/2011 07:00 CDT	
72677	Edit		QLCRA.OTG.PL.Res	Change - Update Actual End	WIRTZ_2	PL	CompNE	Accpt	05/05/2011 07:30 CDT	05/06/2011 14:47 CDT	Other
72922	Edit		QLCRA.OTG.FE.Res	Change - Update Actual End	AUSTIN_1	FE	CompNE	Accpt	05/03/2011 12:57 CDT	05/06/2011 09:55 CDT	Other
72676	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	WIRTZ_1	PL	CompNE	Apprv	05/03/2011 07:01 CDT	05/04/2011 16:22 CDT	Other
72649	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	AUSTIN_1	PL	CompNE	Apprv	05/02/2011 01:00 CDT	05/02/2011 04:00 CDT	Other
72650	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	AUSTIN_2	PL	CompNE	Apprv	05/02/2011 01:00 CDT	05/02/2011 04:00 CDT	Other
72713	Edit		QLCRA.OTG.M1.Res	Submit - Create Outage	FPP_3	M1	Recvd	RatE	04/28/2011 01:00 CDT	05/01/2011 02:37 CDT	Tube Leak
72716	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	WPP_G4	PL	Active	Apprv	04/29/2011 12:01 CDT	06/05/2011 18:00 CDT	Other
72717	Edit		QLCRA.OTG.FR.Res	Submit - Create Outage	GIDEON_1	FR	Active	Accpt	04/27/2011 17:30 CDT	05/04/2011 18:00 CDT	Fuel Limitation/Lack of Fue
47331	Edit		QLCRA.OTG.PL.Res	Submit - Create Outage	INKS	PL	Cancl	Cancl	04/04/2011 08:00 CDT	05/13/2011 17:00 CDT	Other

a. Click in the field of outage/derate you want to submit, field will be highlighted
b. Click on “Submit” – submits outage/derate from PCI to ERCOT
c. Click on “Update”
d. After a successful submission, the “ISO MRID” field will populate with a the corresponding ERCOT ID number

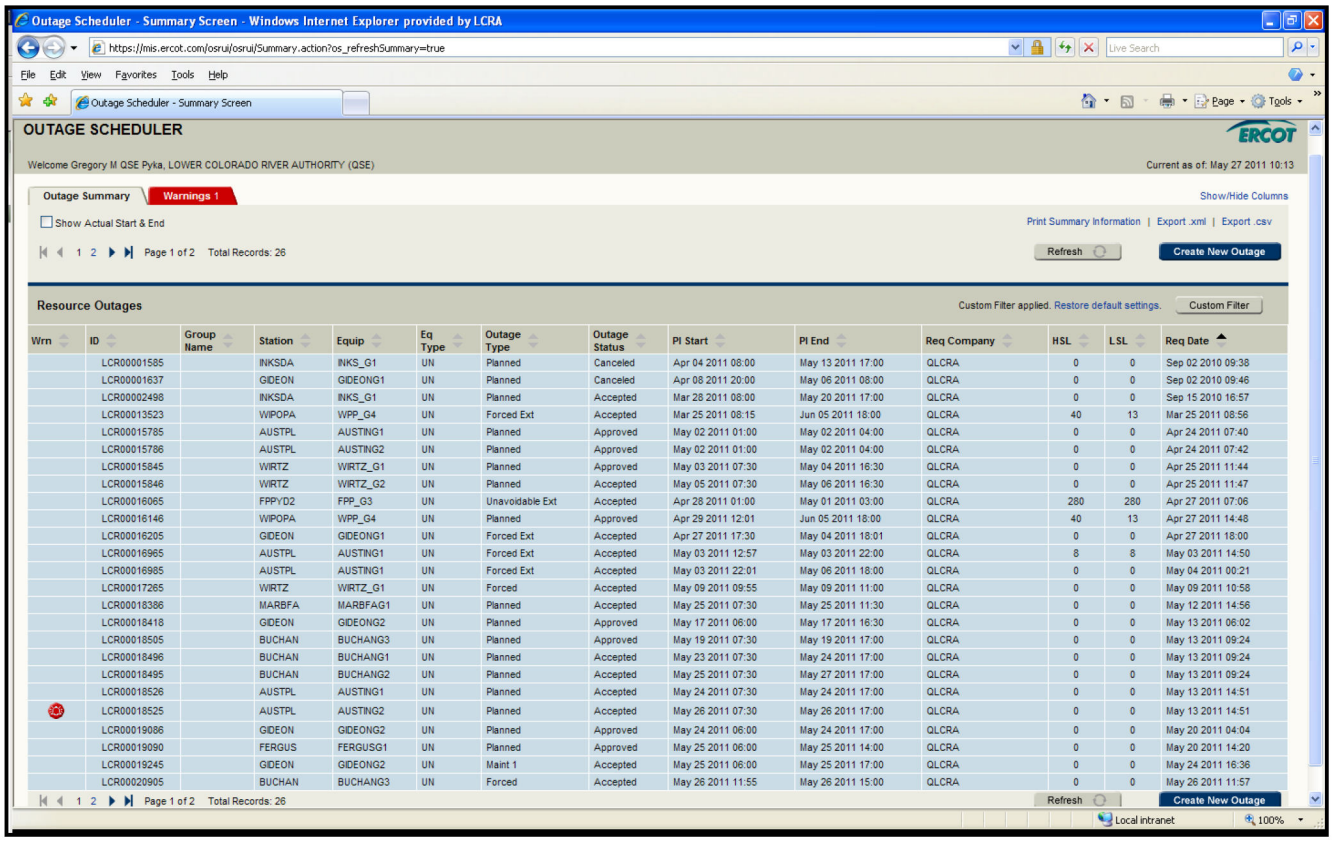
ERCOT Market Information System (MIS)

If PCI is out of service, enter outage in MIS as follows.



ERCOT Market Information System (MIS)

a. Using the appropriate digital certificate to log into MIS
b. Select “Applications”
c. Select “Outage Scheduler”



Wrn	ID	Group Name	Station	Equip	Eq Type	Outage Type	Outage Status	PI Start	PI End	Req Company	HSL	LSL	Req Date
	LCR00001585		INKSDA	INKS_G1	UN	Planned	Canceled	Apr 04 2011 08:00	May 13 2011 17:00	QLCRA	0	0	Sep 02 2010 09:38
	LCR00001637		GIDEON	GIDEONG1	UN	Planned	Canceled	Apr 08 2011 20:00	May 06 2011 08:00	QLCRA	0	0	Sep 02 2010 09:46
	LCR00002498		INKSDA	INKS_G1	UN	Planned	Accepted	Mar 28 2011 08:00	May 20 2011 17:00	QLCRA	0	0	Sep 15 2010 16:57
	LCR00013523		WIPOPA	WPP_G4	UN	Forced Ext	Accepted	Mar 25 2011 08:15	Jun 05 2011 18:00	QLCRA	40	13	Mar 25 2011 08:56
	LCR00015785		AUSTPL	AUSTING1	UN	Planned	Approved	May 02 2011 01:00	May 02 2011 04:00	QLCRA	0	0	Apr 24 2011 07:40
	LCR00015786		AUSTPL	AUSTING2	UN	Planned	Approved	May 02 2011 01:00	May 02 2011 04:00	QLCRA	0	0	Apr 24 2011 07:42
	LCR00015845		WIRTZ	WIRTZ_G1	UN	Planned	Approved	May 03 2011 07:30	May 04 2011 16:30	QLCRA	0	0	Apr 25 2011 11:44
	LCR00015846		WIRTZ	WIRTZ_G2	UN	Planned	Accepted	May 05 2011 07:30	May 06 2011 16:30	QLCRA	0	0	Apr 25 2011 11:47
	LCR00016065		FPPYD2	FPP_G3	UN	Unavoidable Ext	Accepted	Apr 28 2011 01:00	May 01 2011 03:00	QLCRA	280	280	Apr 27 2011 07:06
	LCR00016146		WIPOPA	WPP_G4	UN	Planned	Approved	Apr 29 2011 12:01	Jun 05 2011 18:00	QLCRA	40	13	Apr 27 2011 14:48
	LCR00016205		GIDEON	GIDEONG1	UN	Forced Ext	Accepted	Apr 27 2011 17:30	May 04 2011 18:01	QLCRA	0	0	Apr 27 2011 18:00
	LCR00016965		AUSTPL	AUSTING1	UN	Forced Ext	Accepted	May 03 2011 12:57	May 03 2011 22:00	QLCRA	8	8	May 03 2011 14:50
	LCR00016985		AUSTPL	AUSTING1	UN	Forced Ext	Accepted	May 03 2011 22:01	May 06 2011 18:00	QLCRA	0	0	May 04 2011 00:21
	LCR00017265		WIRTZ	WIRTZ_G1	UN	Forced	Accepted	May 09 2011 09:55	May 09 2011 11:00	QLCRA	0	0	May 09 2011 10:58
	LCR00018386		MARBFA	MARBFAG1	UN	Planned	Accepted	May 25 2011 07:30	May 25 2011 11:30	QLCRA	0	0	May 12 2011 14:56
	LCR00018418		GIDEON	GIDEONG2	UN	Planned	Approved	May 17 2011 06:00	May 17 2011 16:30	QLCRA	0	0	May 13 2011 06:02
	LCR00018505		BUCHAN	BUCHANG3	UN	Planned	Approved	May 19 2011 07:30	May 19 2011 17:00	QLCRA	0	0	May 13 2011 09:24
	LCR00018496		BUCHAN	BUCHANG1	UN	Planned	Accepted	May 23 2011 07:30	May 24 2011 17:00	QLCRA	0	0	May 13 2011 09:24
	LCR00018495		BUCHAN	BUCHANG2	UN	Planned	Accepted	May 25 2011 07:30	May 27 2011 17:00	QLCRA	0	0	May 13 2011 09:24
	LCR00018526		AUSTPL	AUSTING1	UN	Planned	Accepted	May 24 2011 07:30	May 24 2011 17:00	QLCRA	0	0	May 13 2011 14:51
PCI	LCR00018525		AUSTPL	AUSTING2	UN	Planned	Accepted	May 26 2011 07:30	May 26 2011 17:00	QLCRA	0	0	May 13 2011 14:51
	LCR00019086		GIDEON	GIDEONG2	UN	Planned	Approved	May 24 2011 06:00	May 24 2011 17:00	QLCRA	0	0	May 20 2011 04:04
	LCR00019090		FERGUS	FERGUSG1	UN	Planned	Approved	May 25 2011 06:00	May 25 2011 14:00	QLCRA	0	0	May 20 2011 14:20
	LCR00019245		GIDEON	GIDEONG2	UN	Maint 1	Accepted	May 25 2011 06:00	May 25 2011 17:00	QLCRA	0	0	May 24 2011 16:36
	LCR00020905		BUCHAN	BUCHANG3	UN	Forced	Accepted	May 26 2011 11:55	May 26 2011 15:00	QLCRA	0	0	May 26 2011 11:57

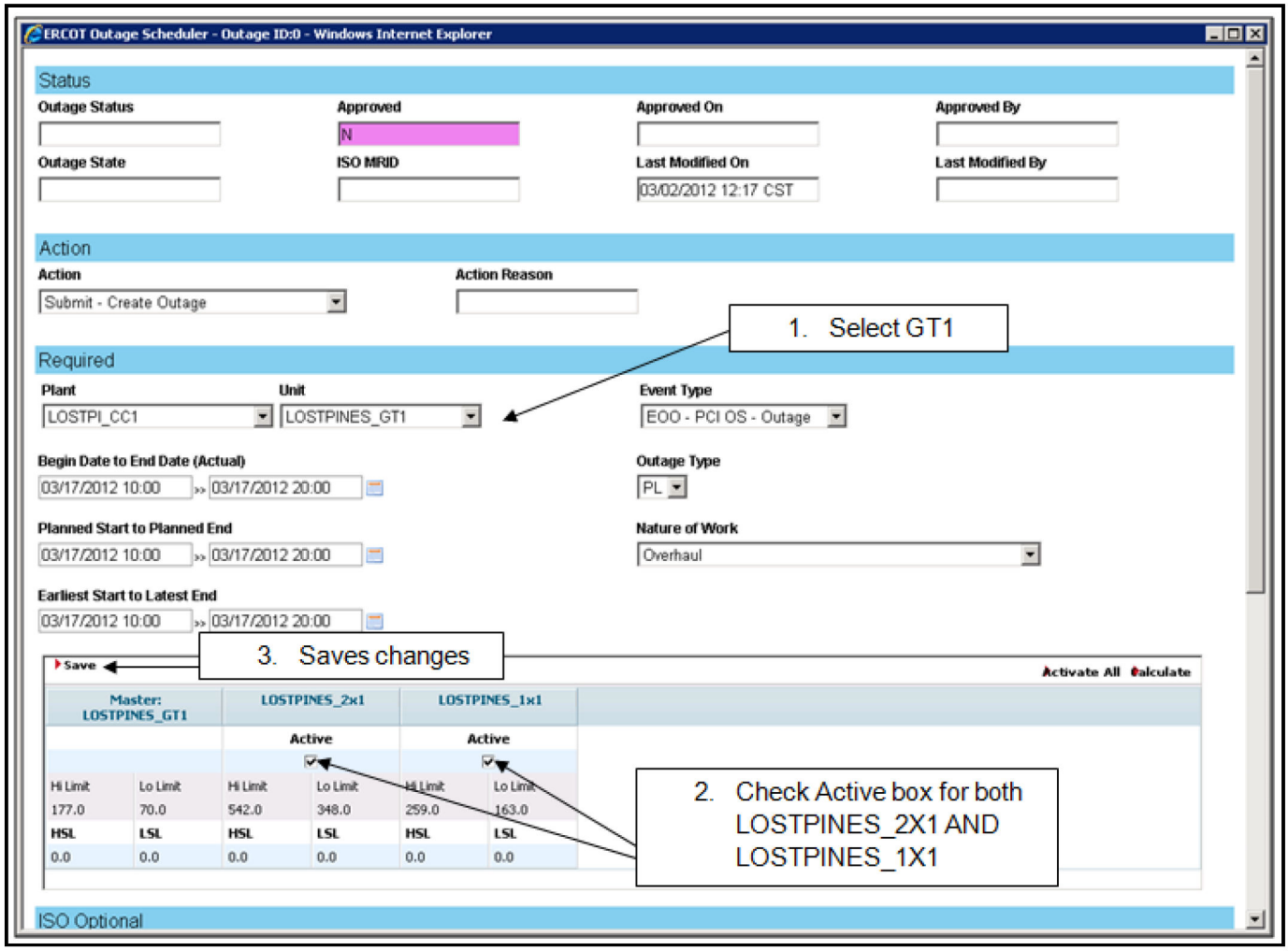
a. "Custom Filter" – choose the appropriate date range, resource, node
b. "Create New Outage" – only use this if PCI system is out of service
c. "Refresh" – displays the latest changes within the outage scheduler

8. Appendix B – Combined Cycle Outage Scheduling in PCI

STEPS:

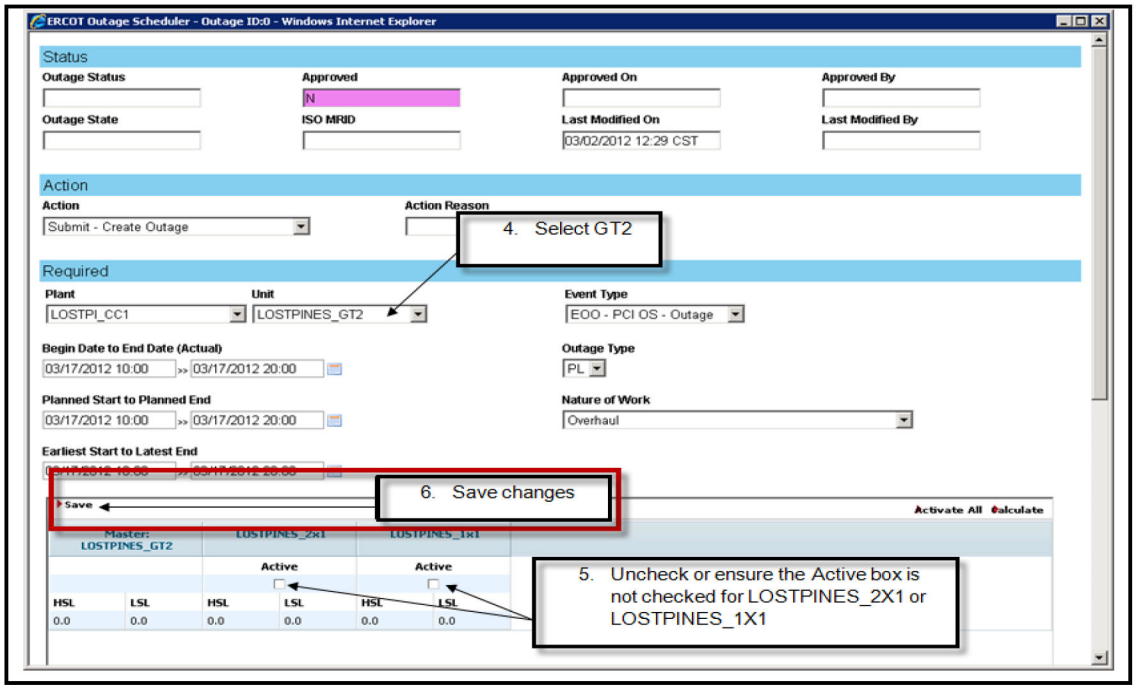
1. Plant requests a GT1, GT2 and ST1 Outage for the same time duration.

1.1 Building the GT1 outage - this will build an EOO unit constraint for GT1 and 2X1 and 1X1 configuration.

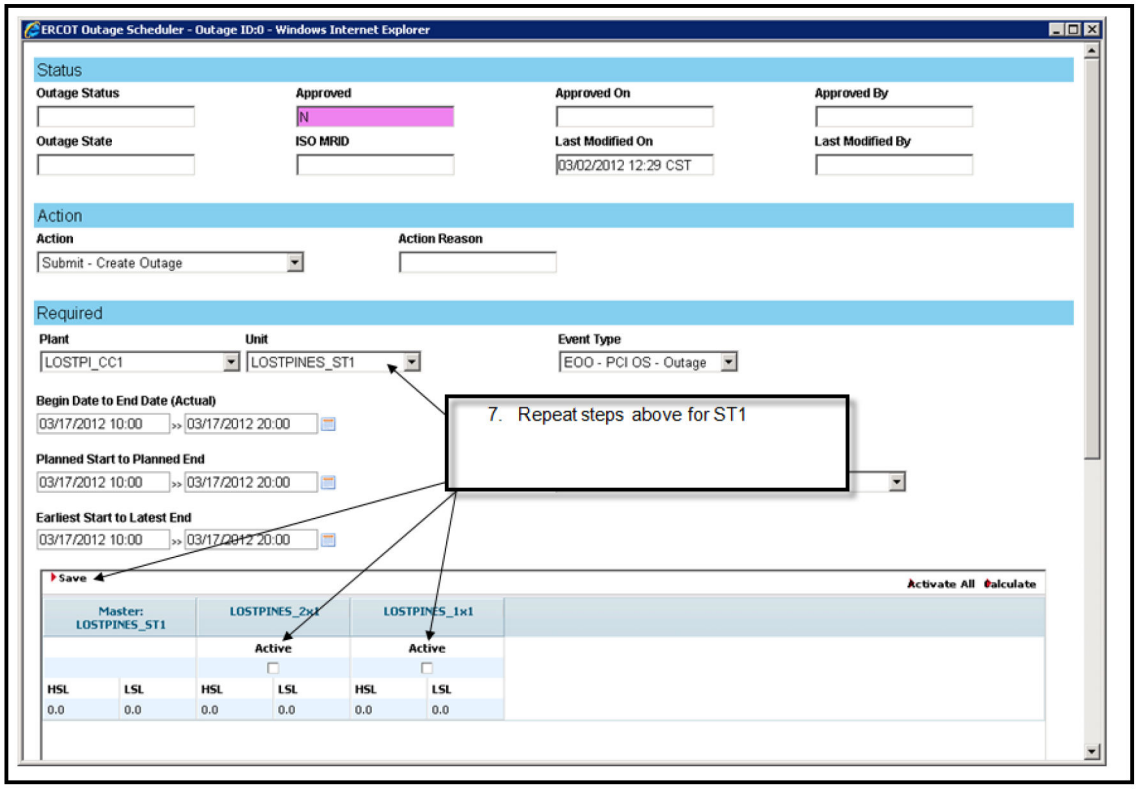


****NOTE** By selecting both "ACTIVE" boxes, you are confirming that the constraint will cause that configuration to be unavailable. You shall leave the box unchecked if the configuration is still available.**

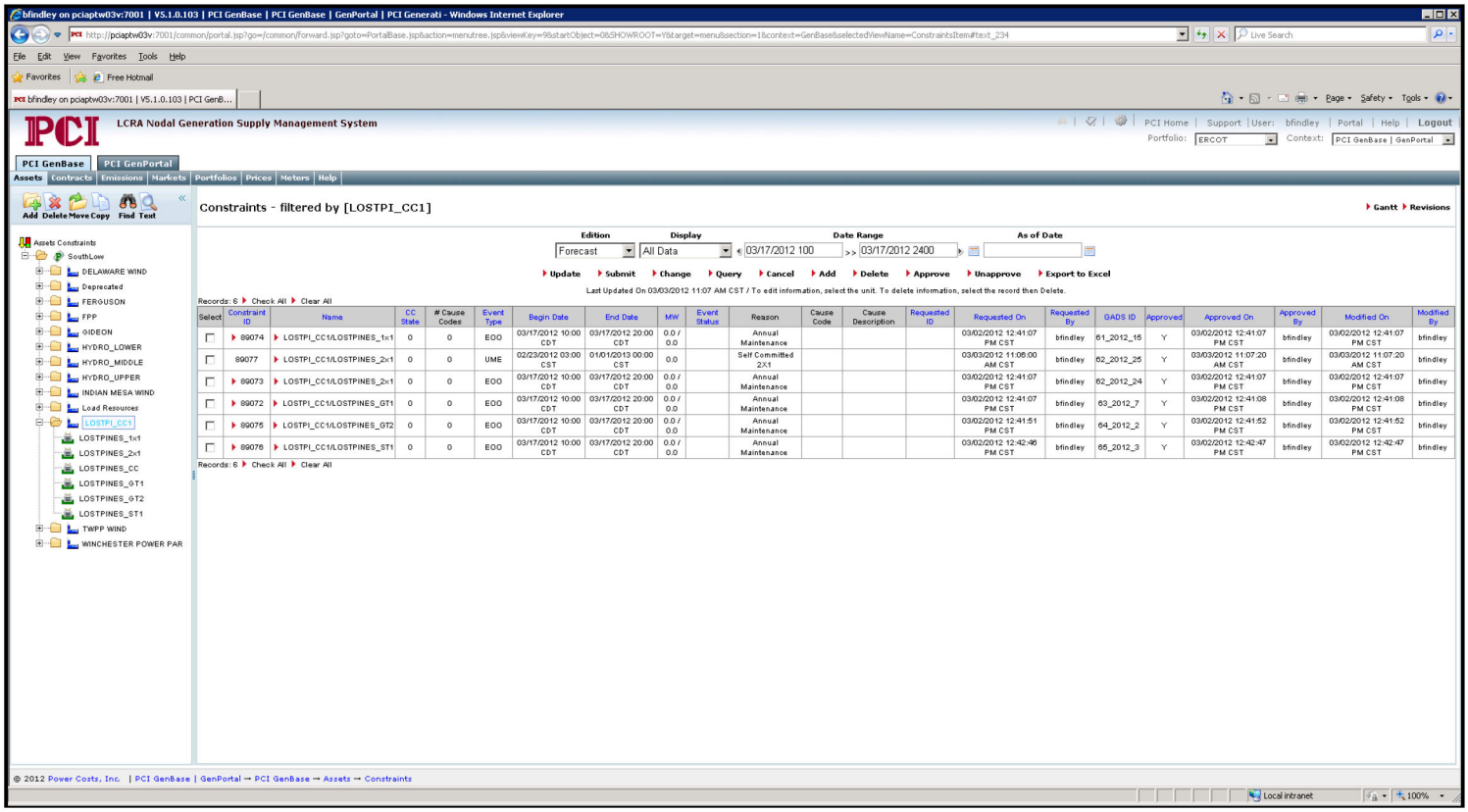
1.2 Building the GT2 outage - this will build an EOO unit constraint for GT2



1.3 Building the ST1 outage- this will build an EOO unit constraint for ST1



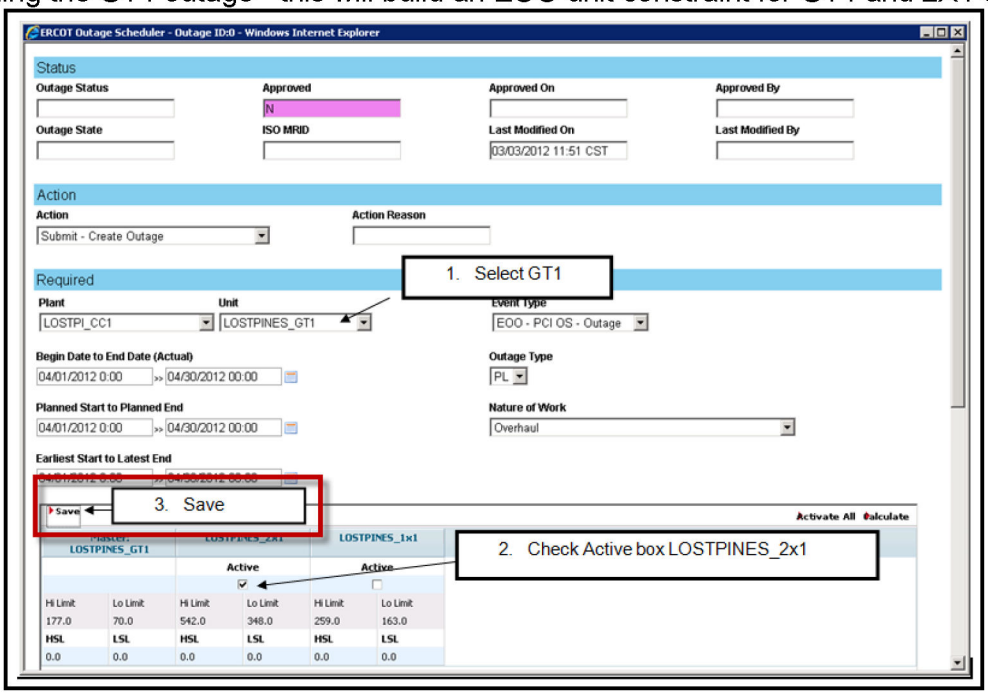
1.4 Below, verify unit constraints are as expected. All of the Lost Pines outage times match for GT1, GT2, ST1, 2X1 and 1X1 EOOs. The existing UME for LOSTPINES_2X1 does not have to be deleted or unapproved; an EOO takes priority over a UME constraint.



This completes building an outage when Lost Pines requires the entire unit out for repairs.

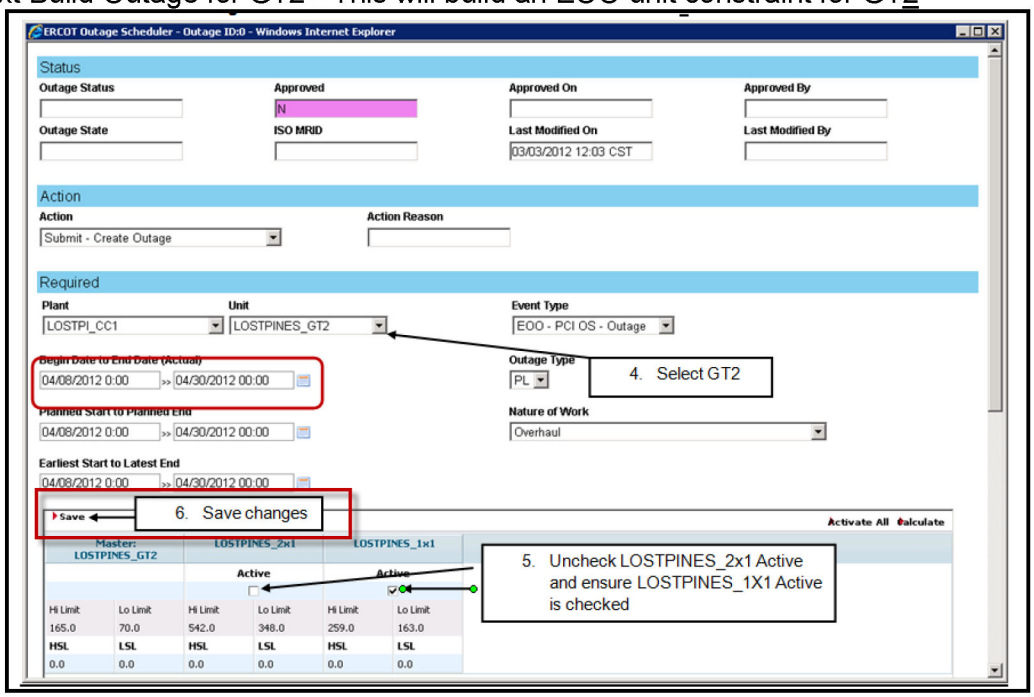
2. Plant requests an outage on GT1, GT2 and ST1, but GT1 outage will begin one week before the complete plant outage and this during time span the plant will run in 1X1 configuration while GT1 is in outage.

2.1 Building the GT1 outage - this will build an EOO unit constraint for GT1 and 2X1 configuration.



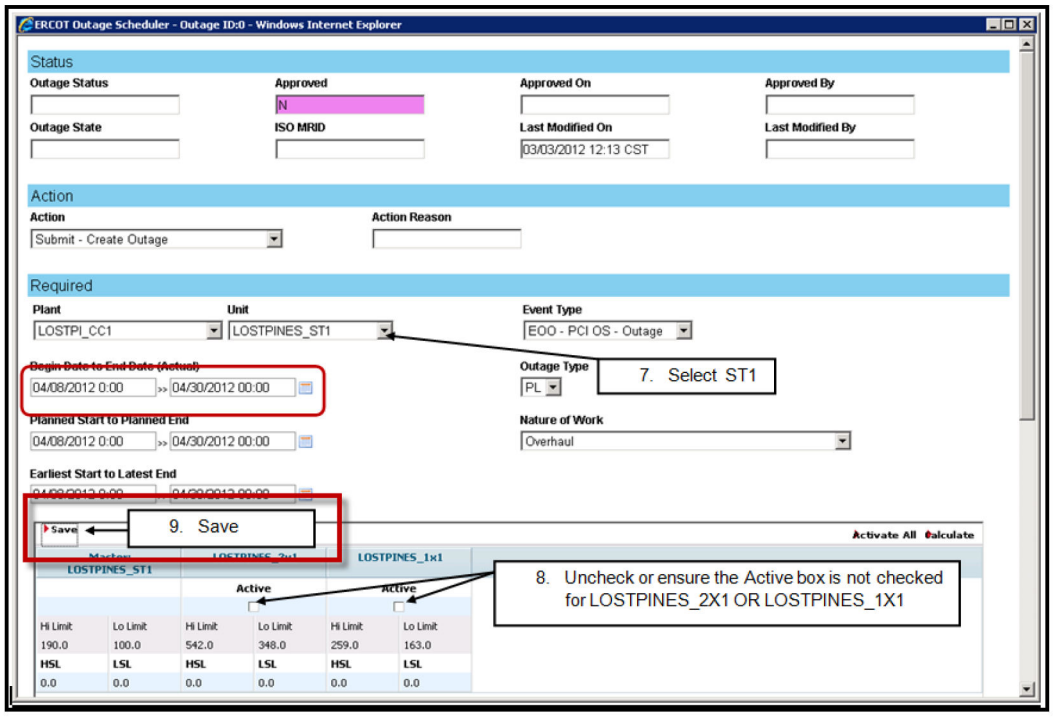
****NOTE** By selecting "ACTIVE" box, you are effectively telling PCI that a 2x1 is not available.**

2.2 Next Build Outage for GT2 - This will build an EOO unit constraint for GT2



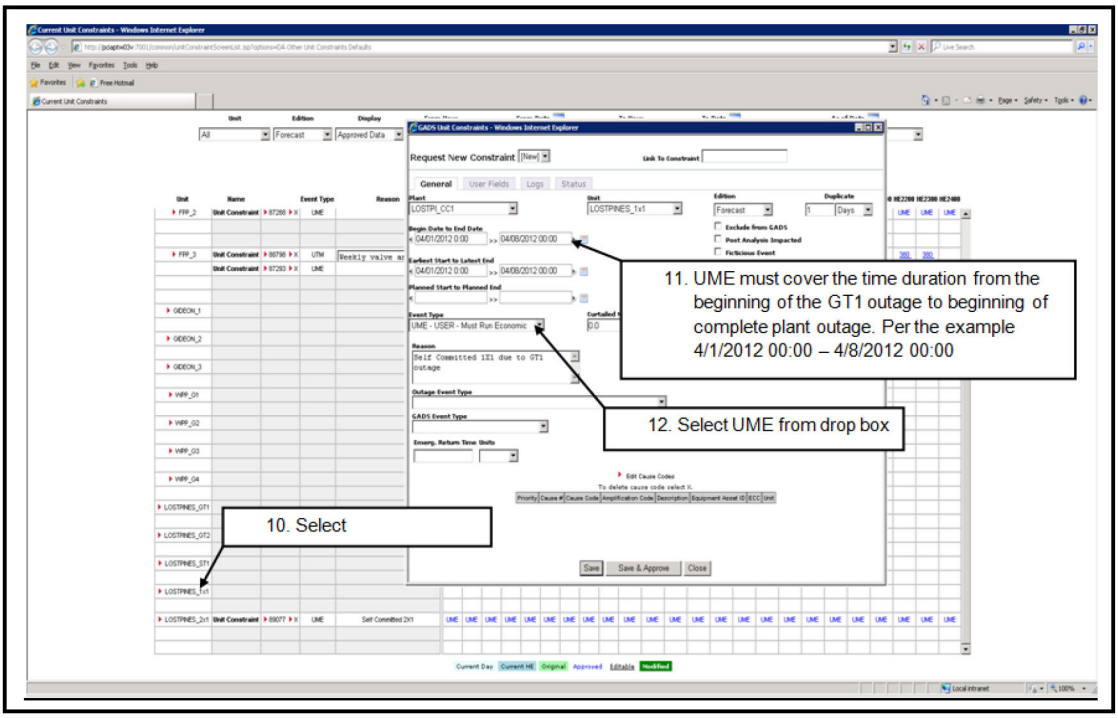
****NOTE** The begin date to end date is different than the GT1 outage built on the previous page.**

2.3 Building the ST1 outage - this will build an EOO unit constraint for ST1

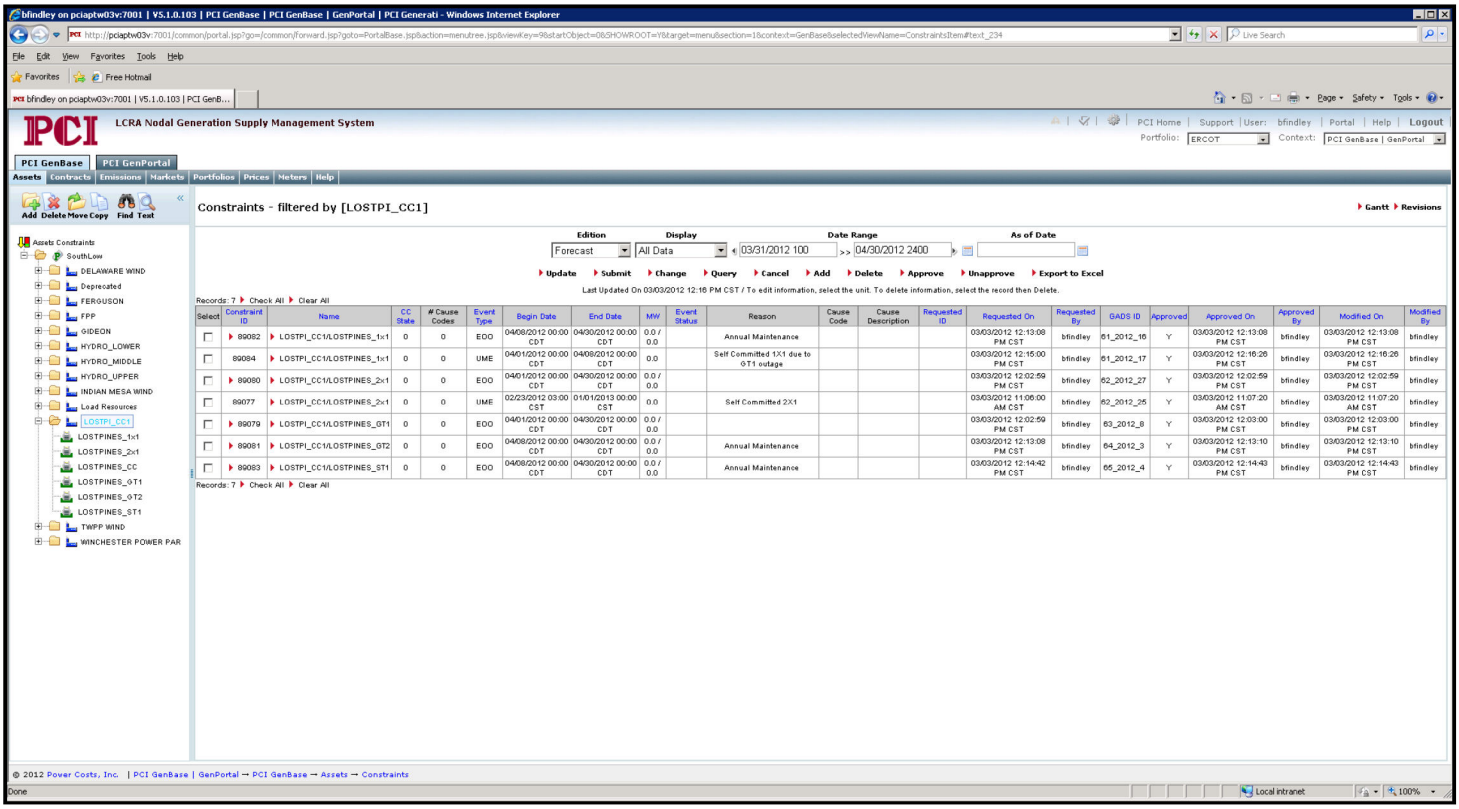


NOTE The begin date to end date is different than the GT1 outage built on the previous page.**

2.4 Once the outages has been entered a UME constraint must be built for the 1X1 Configuration



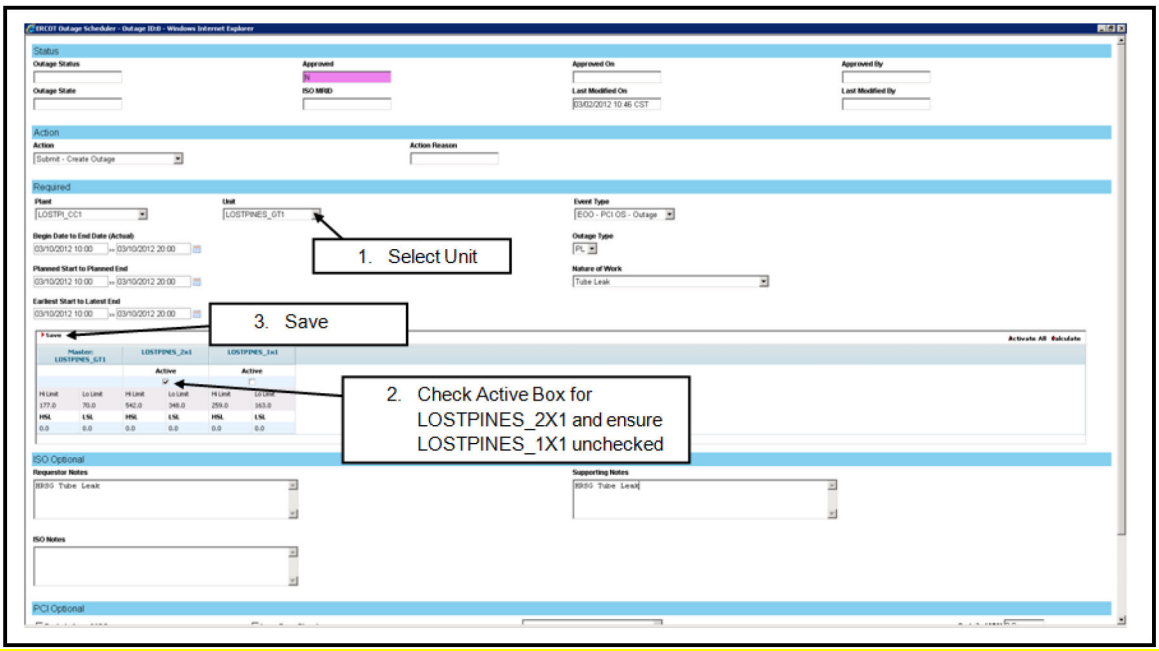
2.5 Below, verify unit constraints are as expected. The Lost Pines outage times match for GT1 and 2X1, additionally the outages times match GT2, ST1 and 1X1 EOOs. There will be an UME for LOSTPINES_1X1 and the existing UME for LOSTPINES_2X1 does not have to be addressed.



This completes building an outage when Lost Pines requires one GT outage prior to a complete unit outage for repairs and unit will run in 1X1 configuration during single GT outage.

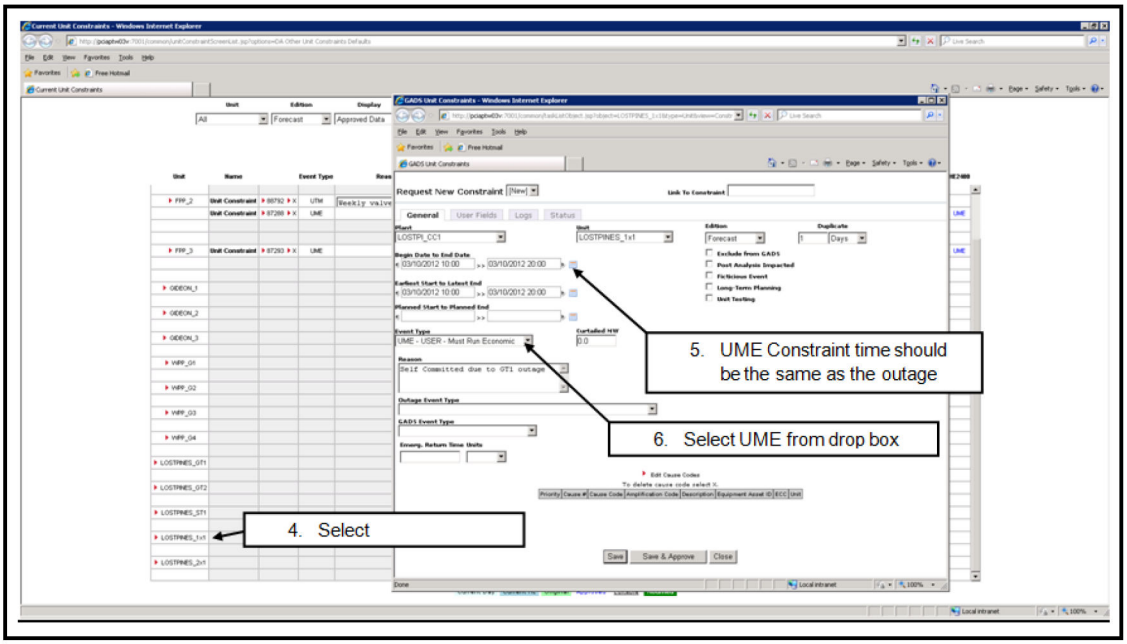
3. Plant requests an outage on one GT and unit will run in a 1X1 configuration for duration of outage.

3.1 Building the GT outage requested - this will build an EOO unit constraint for GT requested

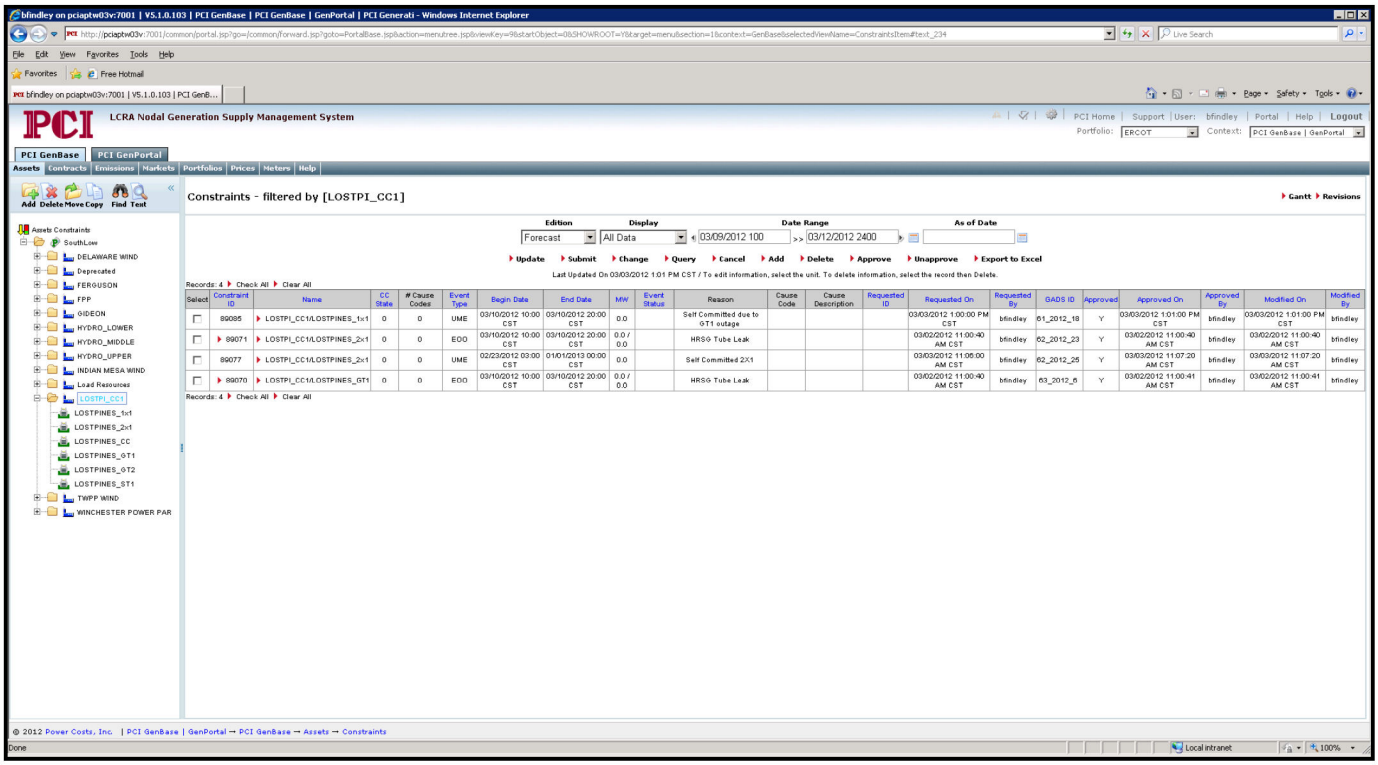


****NOTE** By selecting "ACTIVE" box, you are effectively telling PCI that a 2x1 is not available.**

3.2 Once this outage has been entered, a UME constraint will need to be built for the 1X1 Configuration.



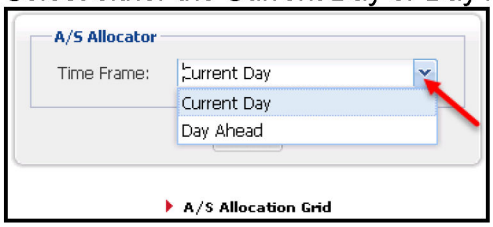
3.3 Below, verify units constraints are as expected. The Lost Pines outage times match for GT1 and 2X1. There will be an UME for LOSTPINES_1X1 and the existing UME for LOSTPINES_2X1 does not have to be addressed.



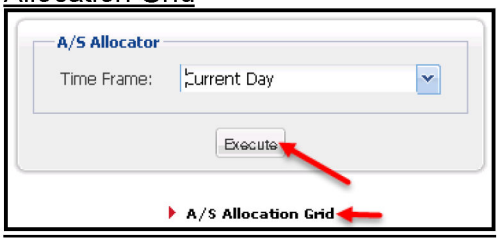
This completes building an outage on one GT and Lost Pines Plant will be running in a 1X1 configuration during outage.

3.4 However, if the GT was committed in the day-ahead market and awarded AS, you will need to reallocate these AS obligations from LOSTPINES 2X1 to LOSTPINES 1X1 and all other committed units.

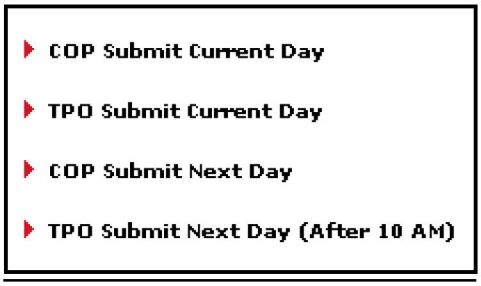
- Select either the Current Day or Day-Ahead on the "A/S Allocator."



- Select Execute and wait until complete. Reallocation of AS can now be viewed by selecting A/S Allocation Grid

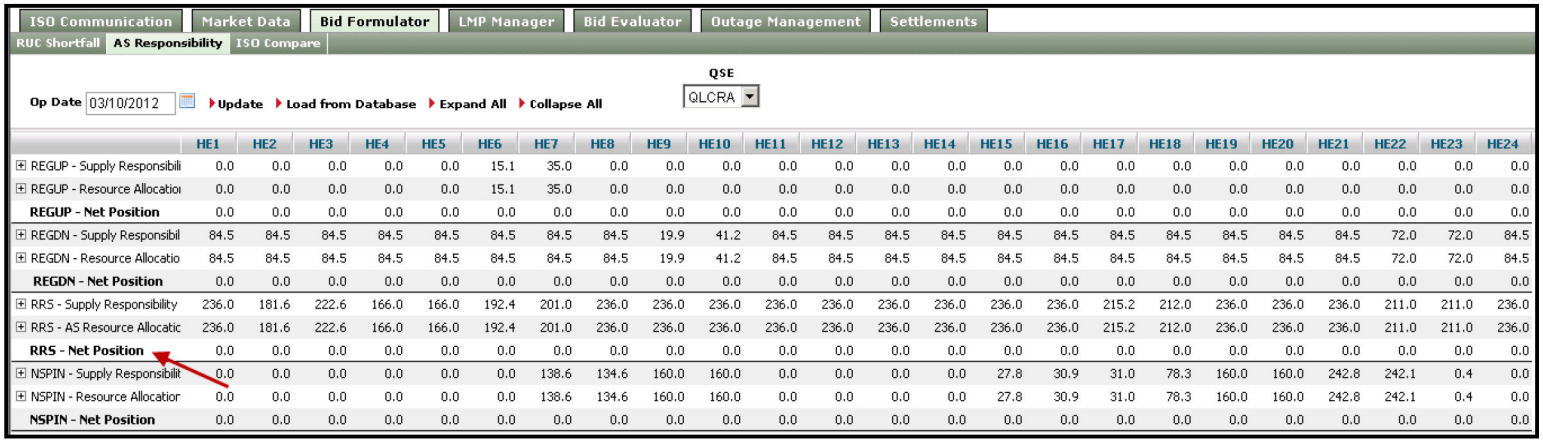


- Select COP Submit then TPO Submit for either current day or next day and verify all COPs and TPOs have been accepted at ERCOT MIS



- GenManager - AS Responsibility

- Check AS Net Positions – in this example, there was enough room on LOSTPINES 1X1 and/or other resources to fully reallocate all AS obligations.

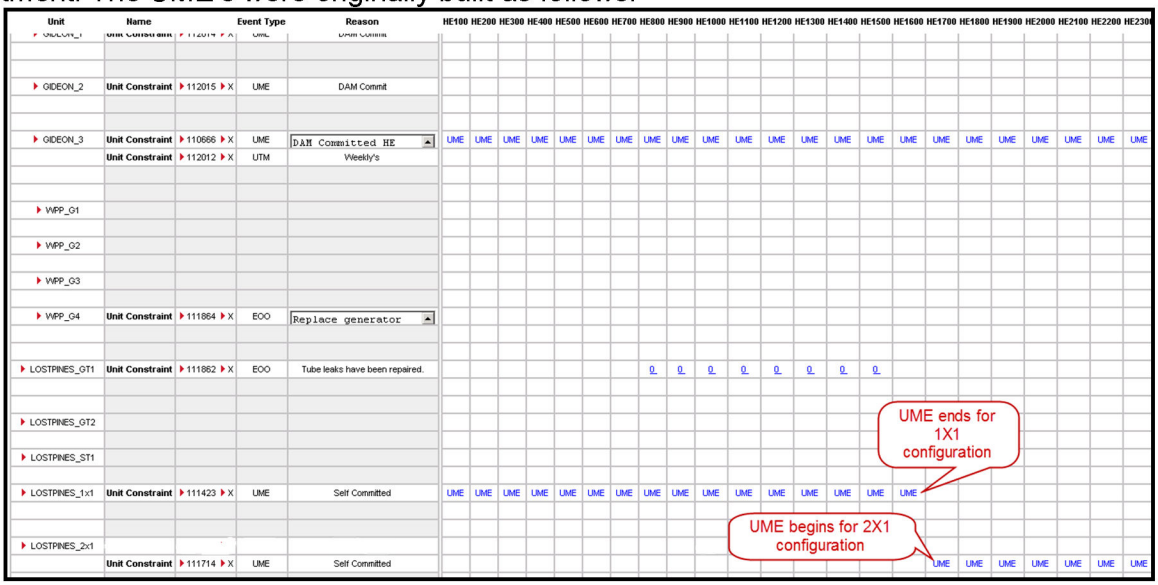


	HE1	HE2	HE3	HE4	HE5	HE6	HE7	HE8	HE9	HE10	HE11	HE12	HE13	HE14	HE15	HE16	HE17	HE18	HE19	HE20	HE21	HE22	HE23	HE24
REGUP - Supply Responsibili	0.0	0.0	0.0	0.0	0.0	15.1	35.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
REGUP - Resource Allocatio	0.0	0.0	0.0	0.0	0.0	15.1	35.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
REGUP - Net Position	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
REGDN - Supply Responsibil	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	19.9	41.2	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	72.0	72.0	84.5
REGDN - Resource Allocatio	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	19.9	41.2	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	84.5	72.0	72.0	84.5
REGDN - Net Position	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
RRS - Supply Responsibility	236.0	181.6	222.6	166.0	166.0	192.4	201.0	236.0	236.0	236.0	236.0	236.0	236.0	236.0	236.0	236.0	215.2	212.0	236.0	236.0	236.0	211.0	211.0	236.0
RRS - AS Resource Allocatic	236.0	181.6	222.6	166.0	166.0	192.4	201.0	236.0	236.0	236.0	236.0	236.0	236.0	236.0	236.0	236.0	215.2	212.0	236.0	236.0	236.0	211.0	211.0	236.0
RRS - Net Position	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
NSPIN - Supply Responsibilit	0.0	0.0	0.0	0.0	0.0	0.0	138.6	134.6	160.0	160.0	0.0	0.0	0.0	0.0	27.8	30.9	31.0	78.3	160.0	160.0	242.8	242.1	0.4	0.0
NSPIN - Resource Allocatior	0.0	0.0	0.0	0.0	0.0	0.0	138.6	134.6	160.0	160.0	0.0	0.0	0.0	0.0	27.8	30.9	31.0	78.3	160.0	160.0	242.8	242.1	0.4	0.0
NSPIN - Net Position	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

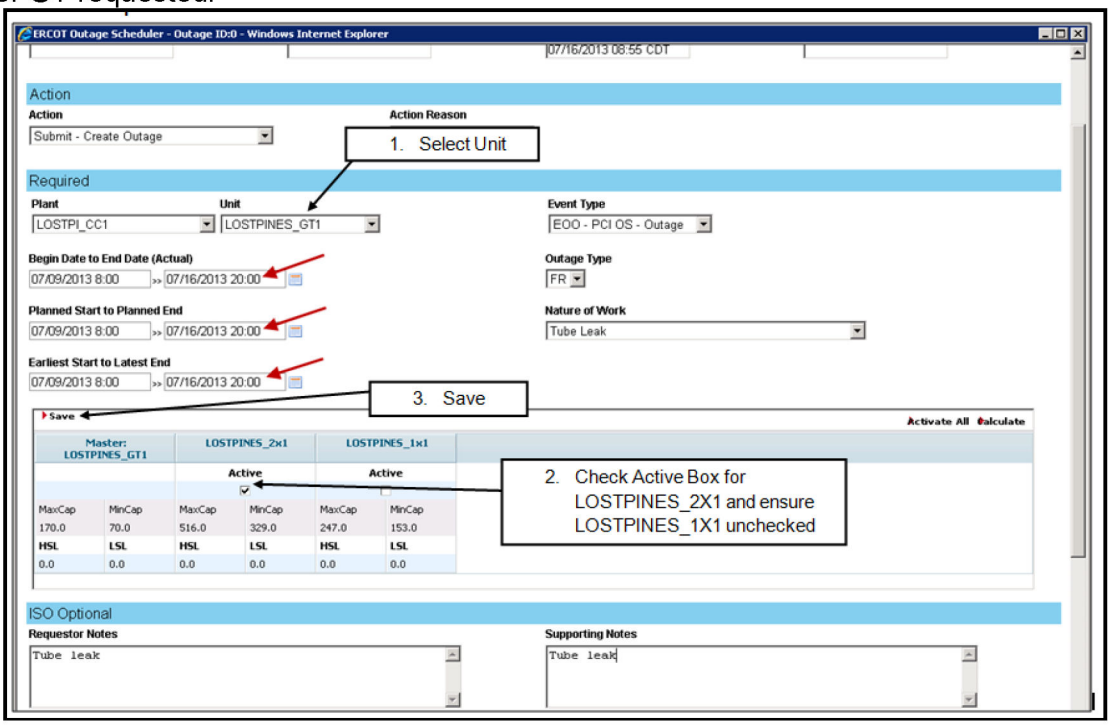
This completes building an outage on one GT and Lost Pines Plant will be running in a 1X1 configuration during outage and reallocating AS.

4. Current configuration on Lost Pines is 1X1. The second GT is offered into the day-ahead market and committed by ERCOT with energy and AS. However, start-up of GT is delayed due to mechanical problems and unit will continue to run in a 1X1 configuration until repairs are completed.

4.1 Transitioning from a 1X1 configuration at HE16:00 to a 2X1 configuration due to day-ahead commitment. The UME's were originally built as follows.

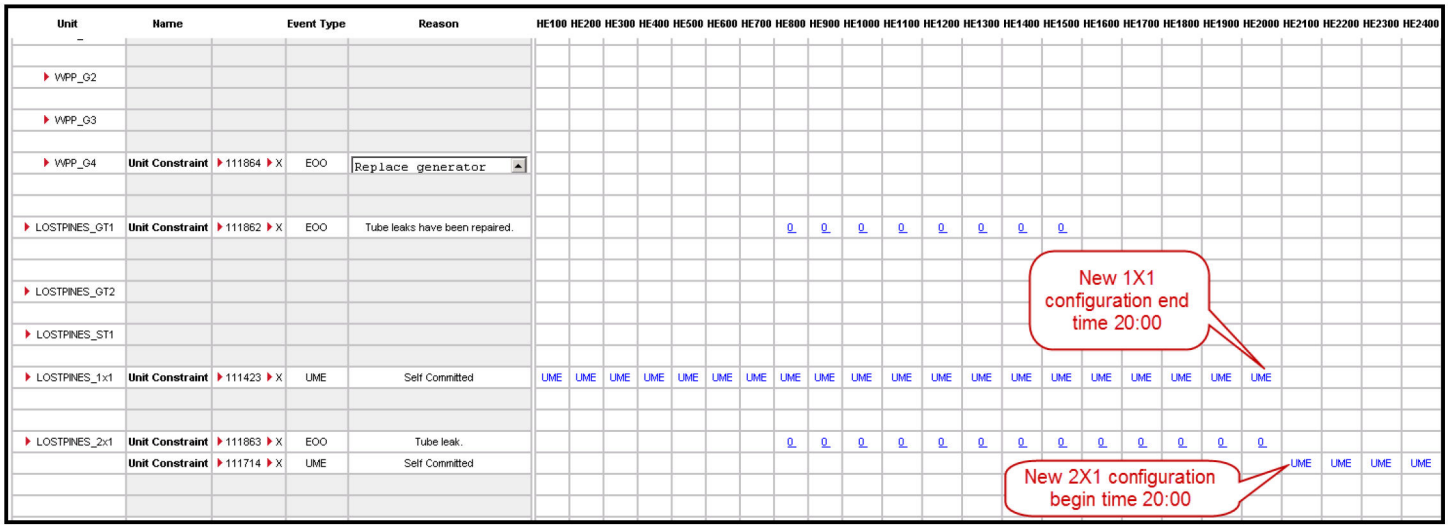


4.2 Due to a delayed start-up, you must build the GT forced outage - this will build an EOO unit constraint for GT requested.

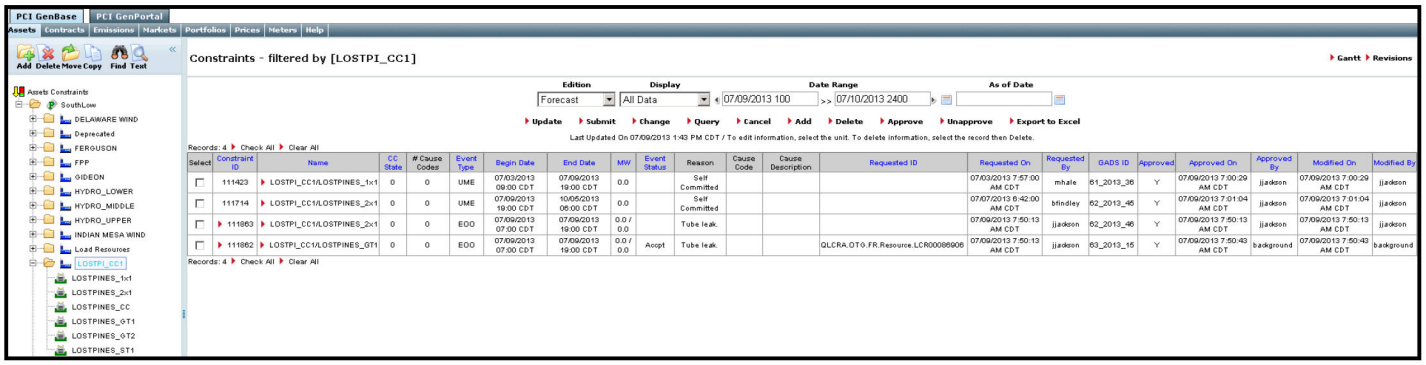


****NOTE** By selecting "ACTIVE" box, you are effectively telling PCI that a 2x1 is not available.**

4.3 Once this forced outage has been entered, the two original UME constraints will need to be modified to reflect the new end time for the 1X1 configuration and new start time for the 2X1 configuration.



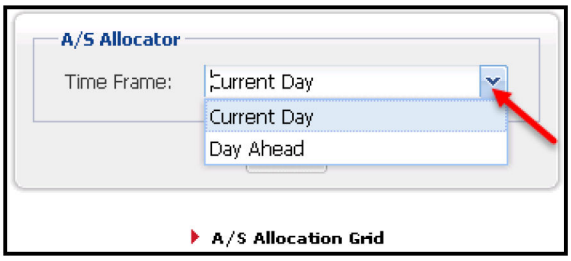
4.4 Below, verify units constraints are as expected. The Lost Pines outage times match for GT1 and 2X1. There will be an UME for LOSTPINES_1X1 and the existing UME for LOSTPINES_2X1.



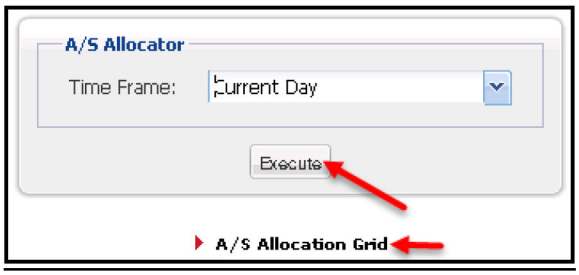
This completes building an outage on one GT and Lost Pines Plant will be running in a 1X1 configuration during outage.

4.5 Since the GT was committed in the day-ahead market and awarded AS for HE17:00-20:00, you must reallocate these AS obligations due to delayed start-up from LOSTPINES 2X1 to LOSTPINES 1X1 and all other committed units.

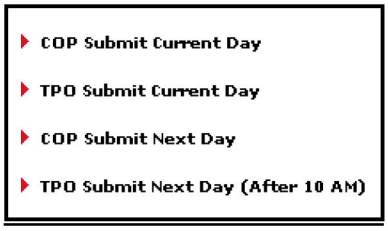
- Select either the Current Day or Day-Ahead on the "A/S Allocator."



- Select Execute and wait until complete. Reallocation of AS can now be viewed by selecting A/S Allocation Grid



- Select COP Submit then TPO Submit for either current day or next day and verify all COPs and TPOs have been accepted at ERCOT MIS



- GenManager - AS Responsibility

- Check AS Net Positions – in this example, there was not enough room on LOSTPINES 1X1 and/or other resources to fully reallocate all AS and now you must inform ERCOT that you are returning (giving back) the 19mw's of RRS.

	HE1	HE2	HE3	HE4	HE5	HE6	HE7	HE8	HE9	HE10	HE11	HE12	HE13	HE14	HE15	HE16	HE17	HE18	HE19	HE20	HE21	HE22	HE23	HE24
⊞ REGUP - Supply Responsibili	69.0	0.0	0.0	0.0	4.5	30.0	30.0	30.0	30.0	30.0	30.0	43.8	99.0	30.0	62.7	99.0	99.0	99.0	51.8	99.0	99.0	99.0	99.0	30.0
⊞ REGUP - Resource Allocatior	69.0	0.0	0.0	0.0	4.5	30.0	30.0	30.0	30.0	30.0	30.0	43.8	99.0	30.0	62.7	99.0	99.0	99.0	51.8	99.0	99.0	99.0	99.0	30.0
REGUP - Net Position	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
⊞ REGDN - Supply Responsibil	39.0	39.0	39.0	39.0	39.0	39.0	39.0	20.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	13.4	39.0
⊞ REGDN - Resource Allocatio	39.0	39.0	39.0	39.0	39.0	39.0	39.0	20.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	13.4	39.0
REGDN - Net Position	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
⊞ RRS - Supply Responsibility	276.0	276.0	267.5	236.0	236.0	276.0	276.0	276.0	330.0	268.4	354.0	276.0	276.0	276.0	276.0	190.0	139.0	131.0	144.0	240.0	276.0	276.0	350.0	276.0
⊞ RRS - AS Resource Allocatic	276.0	276.0	267.5	236.0	236.0	276.0	276.0	276.0	330.0	249.4	354.0	276.0	276.0	276.0	276.0	190.0	139.0	131.0	144.0	240.0	276.0	276.0	350.0	276.0
RRS - Net Position	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	-19.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
⊞ NSPIN - Supply Responsibilit	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	164.7	164.7	150.0	150.0	150.0	150.0	150.0	150.0	150.0
⊞ NSPIN - Resource Allocatior	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	150.0	164.7	164.7	150.0	150.0	150.0	150.0	150.0	150.0	150.0
NSPIN - Net Position	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

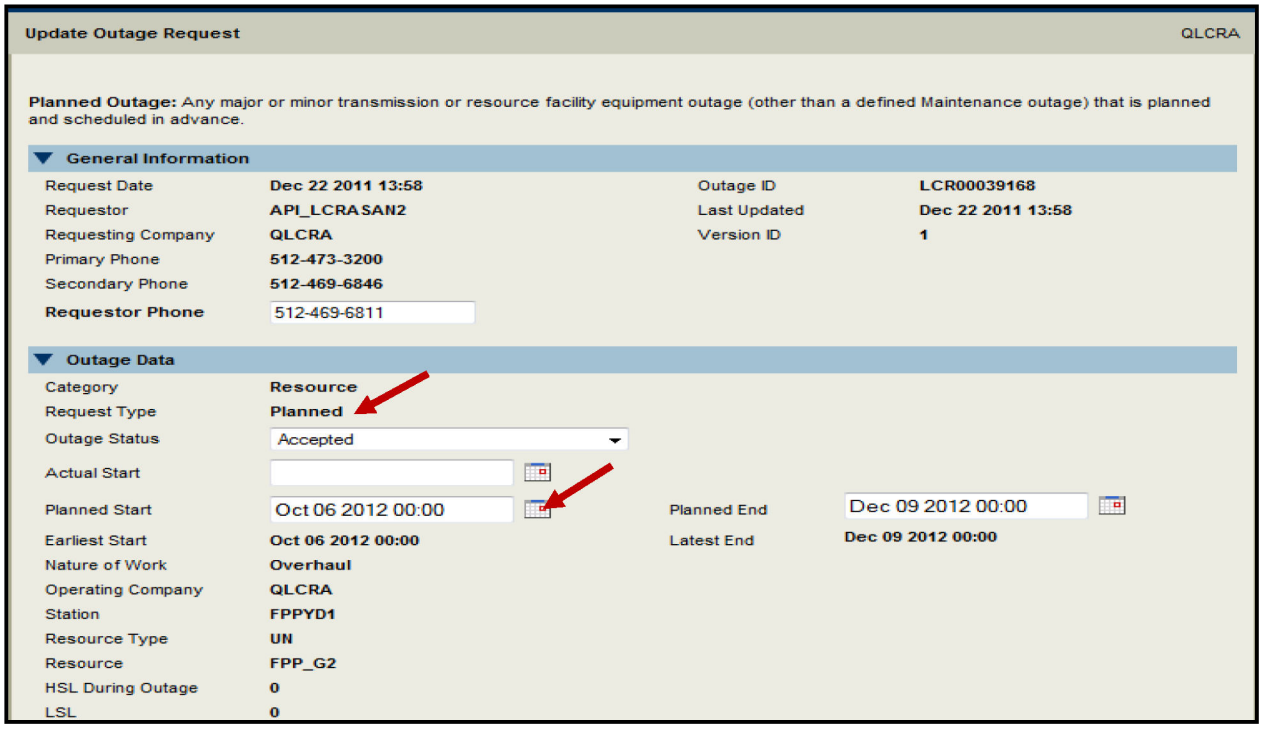
This completes building a forced outage on one GT and Lost Pines Plant will be running in a 1X1 configuration and reallocating AS.

9. Appendix C – ERCOT Outage Coordination Organization

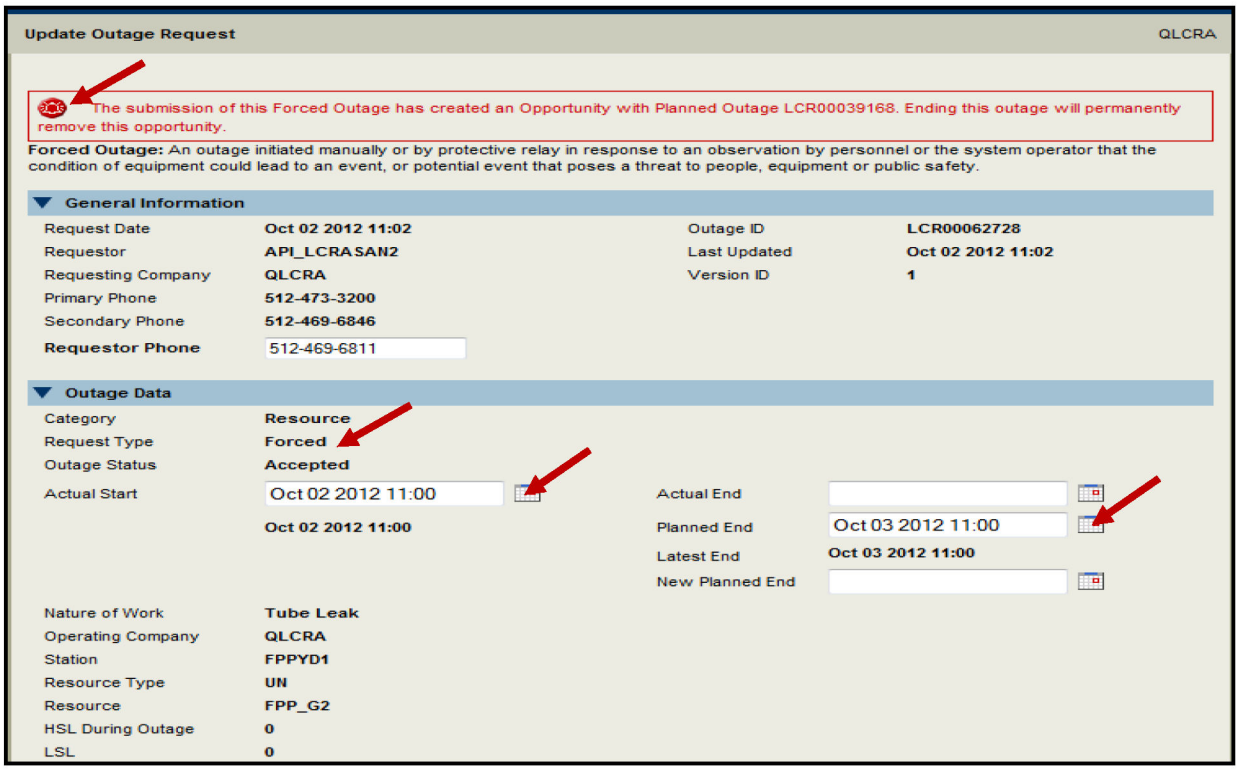
ERCOT Outage Coordination		Phone Number/OPX	Email addresses
		Taylor: 512-248-6841 / 6842	
Bobby Reed	**MGR**	**512-248-4285**	breed@ercot.com
Robert Matlock (Long Term)	**SUPV**	**512-248-3005**	rmatlock@ercot.com
Jay Hawkins (45-90 & >90 Day)	OC	512-248-6983	jhawkins@ercot.com
Shane Thomas (9-45 Day)	E	512-248-3813	sthomas@ercot.com
Alex Lee	E	512-248-4287	alee@ercot.com
Rusty Dawson (9-45 Day)	OC	512-248-4652	rdawson@ercot.com
David Tucker (9-45 Day)	OC	512-248-4664	dtucker@ercot.com
Angie Moy (Res Trans)	OCA	512-248-6627	amoy@ercot.com
Diane Simons (Resource)	OC	512-248-4282	dsimons@ercot.com
Darrell Jenkins (Short-Term)	**SUPV**	**512-248-6846**	djenkins@ercot.com
Randy Wind (3-4 Day)	OC	512-248-3939	rwind@ercot.com
Phil Sanford (3-4 Day)	OC	512-248-3138	psanford@ercot.com
Jerry Vinson (3-4 Day)	OC	512-248-3899	jvinson@ercot.com
Bill Dillow (3-4 Day)	OC	512-248-4291	bdillow@ercot.com
Ed Mercado (3-4 Day)	OC	512-248-3991	emercado@ercot.com

ERCOT Outage Coordination	Phone Number	Email
	512-248-6841	opsoutagecoordination@ercot.com

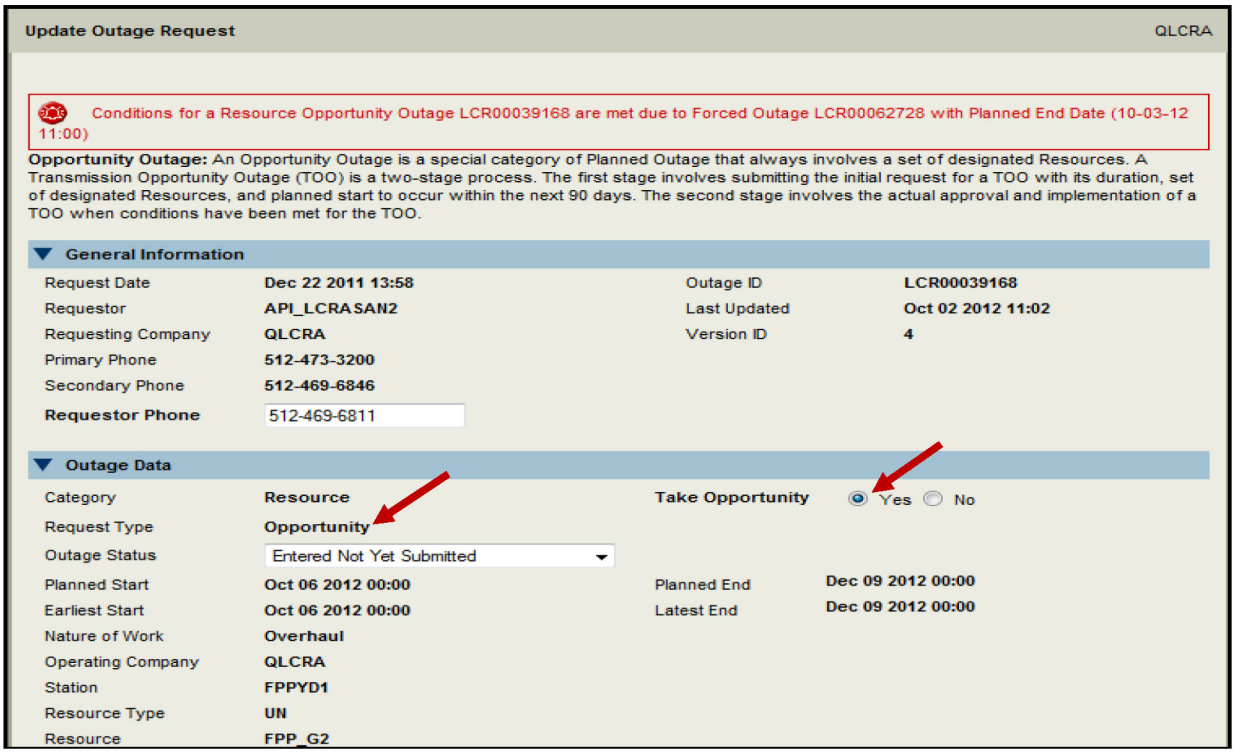
10. Appendix D - ERCOT Outage Scheduler – Opportunity Outage



Submitted Forced Outage in ERCOT Outage Scheduler to begin October 2 and end October 3. Note the red warning that an Opportunity Outage has been created because it falls within the 8 day criteria.

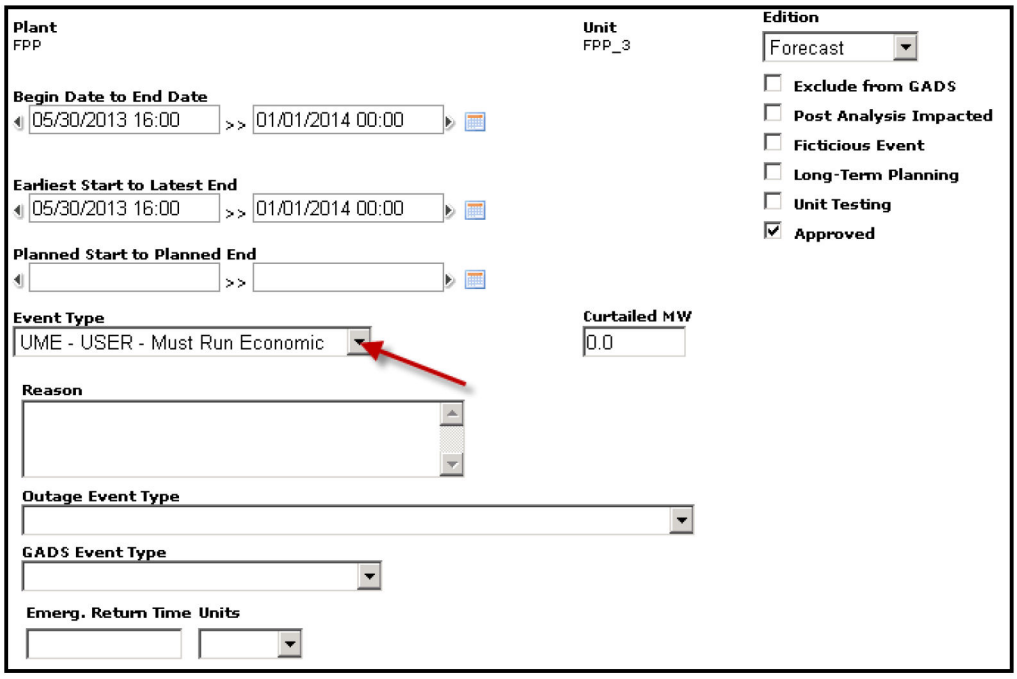


The original “Request Type” Planned Outage has now changed to Opportunity when you submitted the Forced Outage. Select “Yes” if it’s decided to start Planned Outage earlier than scheduled.

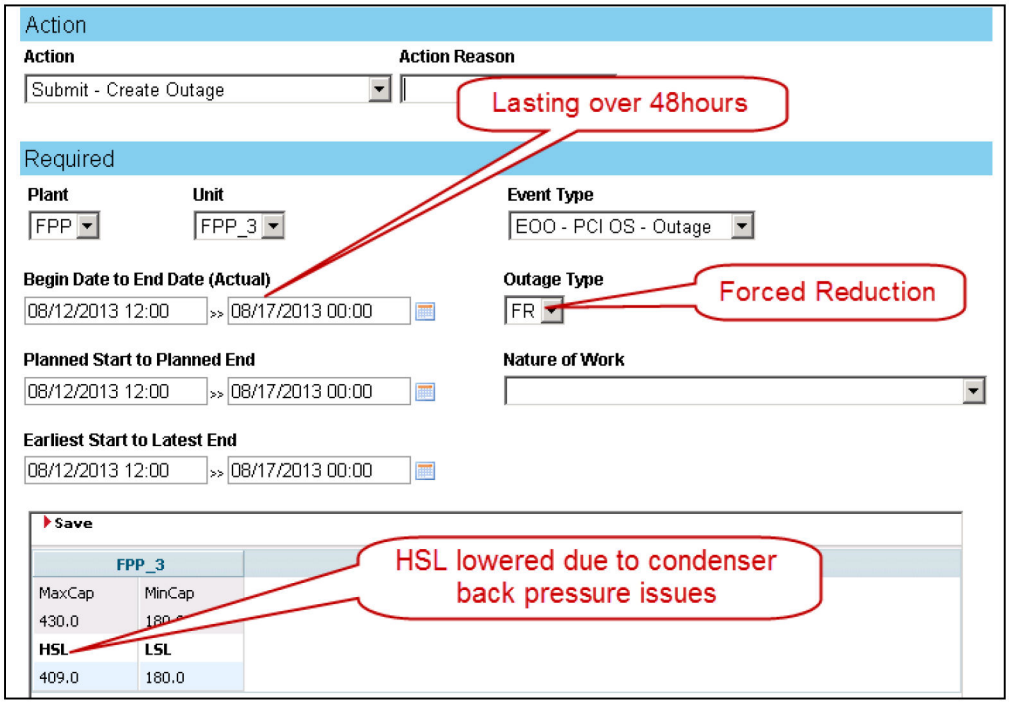


11. Appendix E – Multiple Derates on a Single Resource

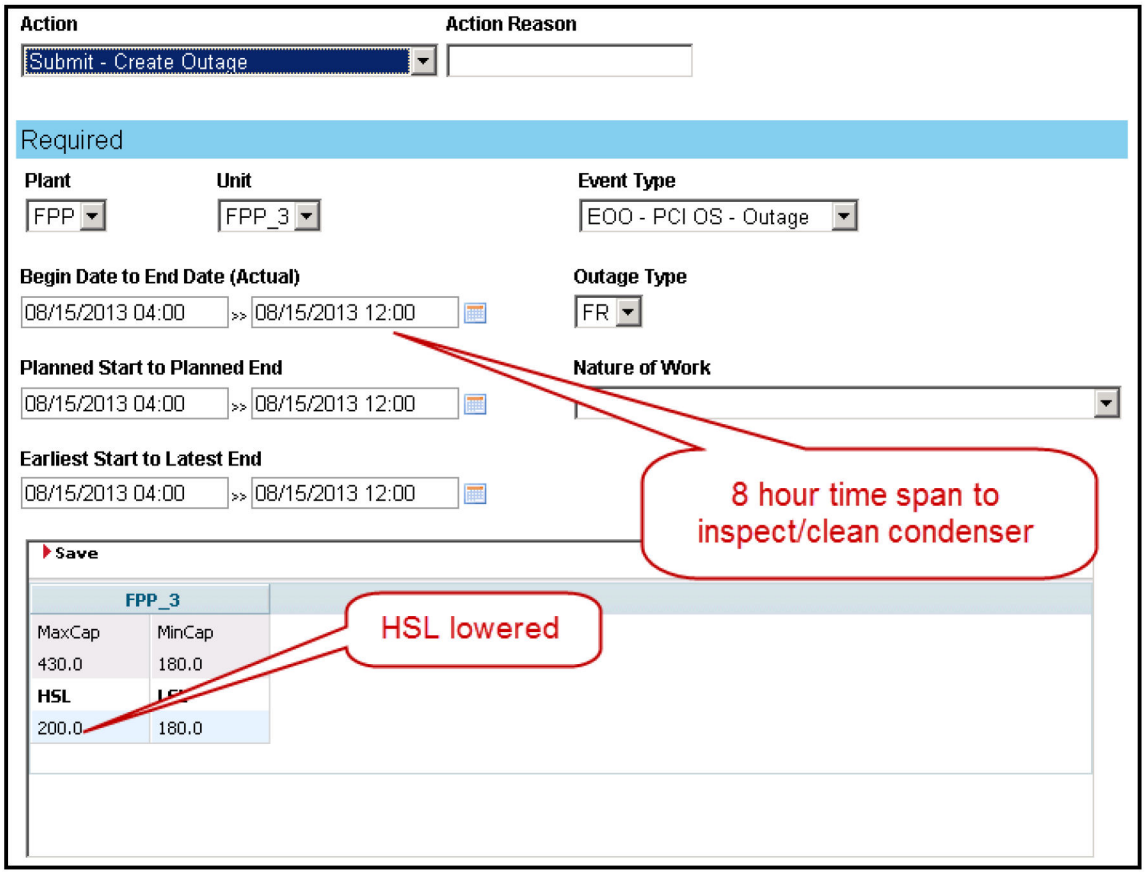
1. Example, FPP-3 has the standard original UME (must run economic) built for the entire year.



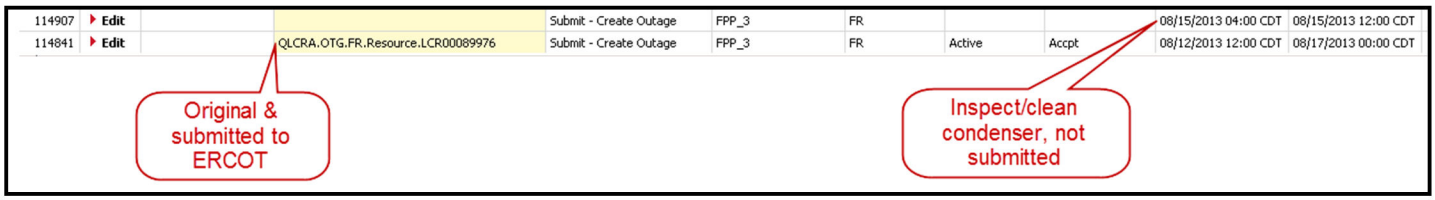
2. Due to back pressure problems with the condenser, FPP-3 is was derated to 409mw's for 4½ days. Derate is built in PCI outage scheduler and submitted to ERCOT. Remember, any derate lasting longer than 48 hours and greater than 5% of its seasonal HSL must be reported to ERCOT.



3. The maintenance department decides to do an inspection and cleaning on the condenser so they request one side to be taken out of service for an 8 hour period which will further limit the resource to 200mw's. Instead of modifying and ending the original derate at the begin time of the new derate then building another derate to start at the end of the maintenance period, it would simply be easier to leave the original derate alone and build a second derate from Outage Scheduler for the short maintenance window but DO NOT submit it to ERCOT. This second derate will have to built as a FR or M1 Event Type in order for the new HSL to appear in the COP.



4. PCI Outage Scheduler



5. COP in GenManager

Current Operating Plan | Output Schedule | Inc/Dec Offer | Three Part Offer | A/S Offer

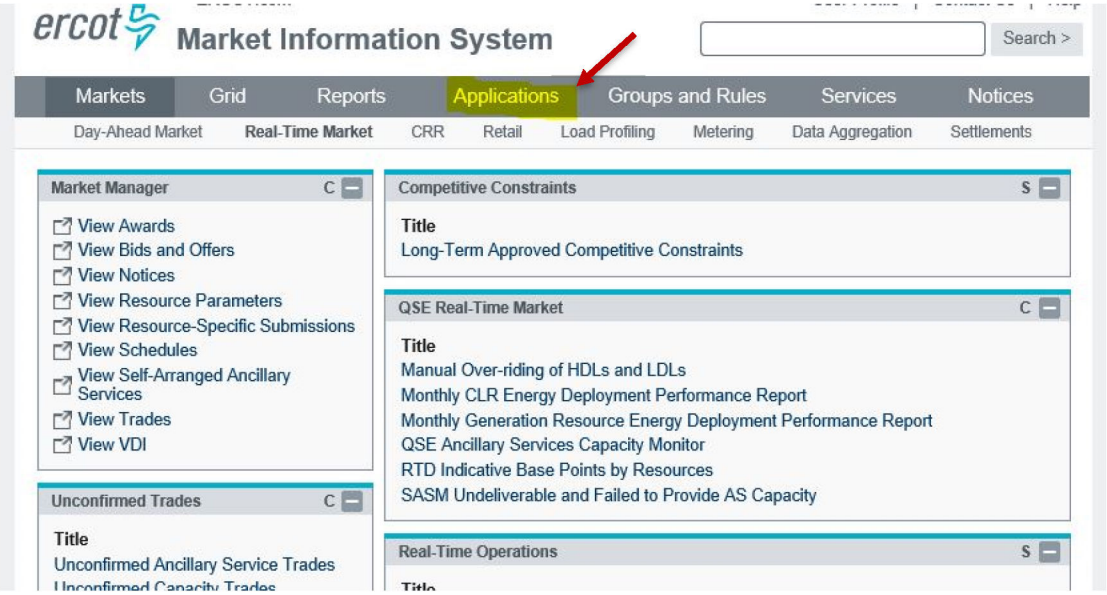
Location Name	Select	HE	LEL	LSL	HSL	HEL	Reg-Up	Reg-Down	RRS	Non-Spin	Unit Status
FPP 3	☐	1	180.0	180.0	409.0	409.0	0.0	0.0	0.0	0.0	ON
		2	180.0	180.0	409.0	409.0	0.0	0.0	0.0	0.0	ON
		3	180.0	180.0	409.0	409.0	0.0	0.0	0.0	0.0	ON
		4	180.0	180.0	409.0	409.0	0.0	0.0	0.0	0.0	ON
		5	180.0	180.0	200.0	200.0	0.0	0.0	0.0	0.0	ON
		6	180.0	180.0	200.0	200.0	0.0	0.0	0.0	0.0	ON
		7	180.0	180.0	200.0	200.0	0.0	0.0	0.0	0.0	ON
		8	180.0	180.0	200.0	200.0	0.0	0.0	0.0	0.0	ON
		9	180.0	180.0	200.0	200.0	0.0	0.0	0.0	0.0	ON
		10	180.0	180.0	200.0	200.0	0.0	0.0	0.0	0.0	ON
		11	180.0	180.0	200.0	200.0	0.0	0.0	0.0	0.0	ON
		12	180.0	180.0	200.0	200.0	0.0	0.0	0.0	0.0	ON
		13	180.0	180.0	409.0	409.0	0.0	0.0	30.0	0.0	ON
		14	180.0	180.0	409.0	409.0	0.0	0.0	15.0	0.0	ON
		15	180.0	180.0	409.0	409.0	0.0	0.0	15.0	0.0	ON
		16	180.0	180.0	409.0	409.0	0.0	0.0	15.0	0.0	ON
		17	180.0	180.0	409.0	409.0	0.0	0.0	15.0	0.0	ON
		18	180.0	180.0	409.0	409.0	0.0	0.0	15.0	0.0	ON
		19	180.0	180.0	409.0	409.0	0.0	0.0	15.0	0.0	ON
		20	180.0	180.0	409.0	409.0	0.0	0.0	30.0	0.0	ON
		21	180.0	180.0	409.0	409.0	0.0	0.0	30.0	0.0	ON
		22	180.0	180.0	409.0	409.0	0.0	0.0	30.0	0.0	ON
		23	180.0	180.0	409.0	409.0	0.0	0.0	30.0	0.0	ON
		24	180.0	180.0	409.0	409.0	0.0	0.0	0.0	0.0	ON

6. All three derate constraints are active and visible below.

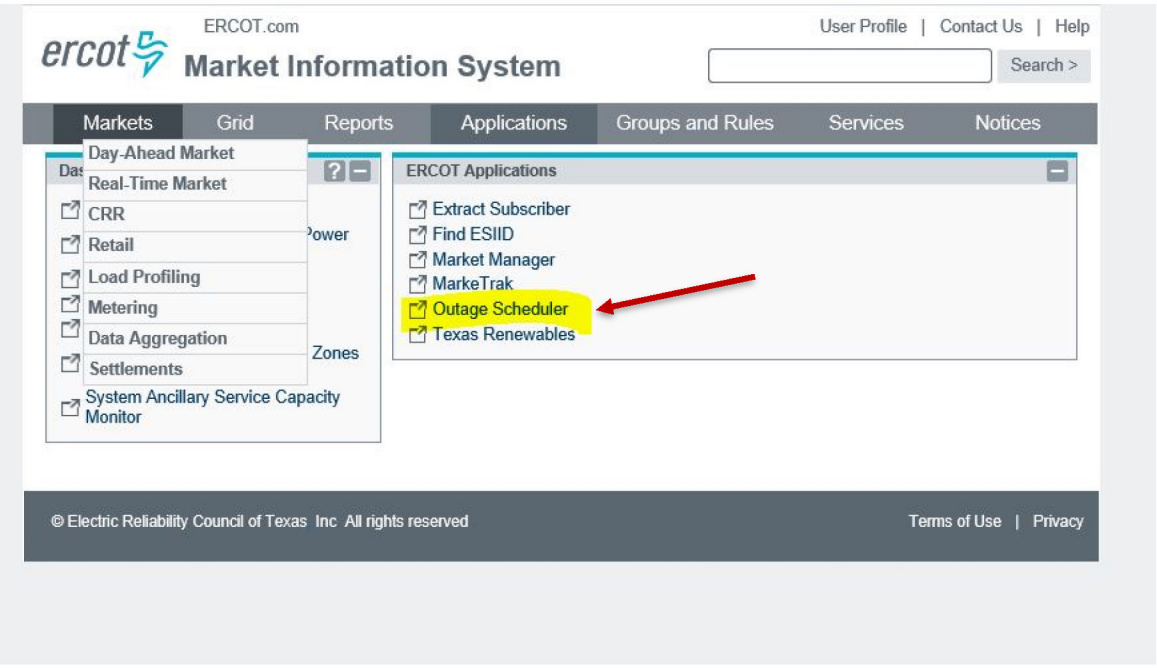
Unit	Name		Event Type	Reason	HE100	HE200	HE300	HE400	HE500	HE600	HE700	HE800	HE900	HE1000	HE1100	HE1200	HE1300	HE1400
FPP_3	Unit Constraint	114841 X	EOO	Condenser issues.	409	409	409	409	409	409	409	409	409	409	409	409	409	409
	Unit Constraint	114907 X	EOO	Condenser Inspection Cleaning					200	200	200	200	200	200	200	200		
	Unit Constraint	108390 X	UME		UME	UME	UME	UME	UME	UME	UME	UME	UME	UME	UME	UME	UME	UME

12. Appendix F – Entering Transmission Equipment Outages

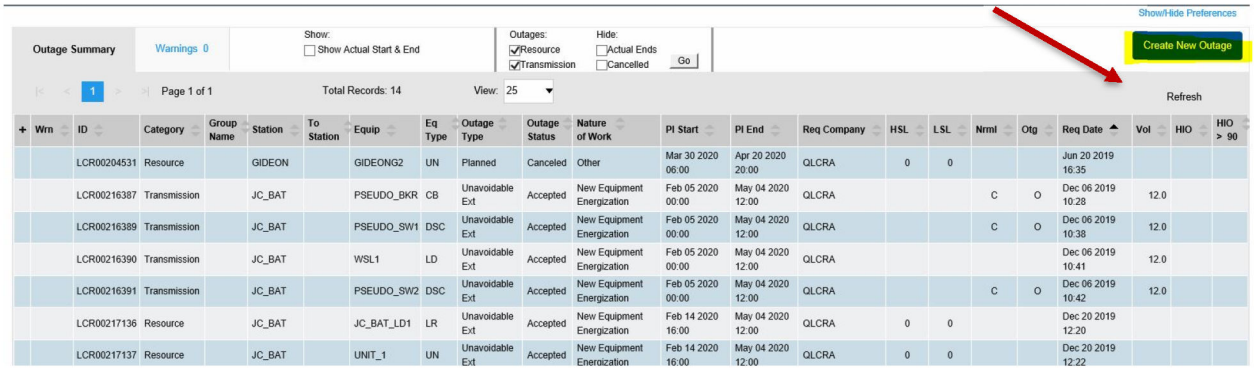
1. In the event that the GenDesk is required to enter transmission elements into the ERCOT Outage Scheduler, use the following steps to accomplish this. Transmission elements cannot be submitted through PCI so the first step will be to navigate to the ERCOT outage scheduler. Begin by opening the ERCOT MSI and locating the Applications Tab.



2. Click on the Applications tab and locate the Outage Scheduler icon.

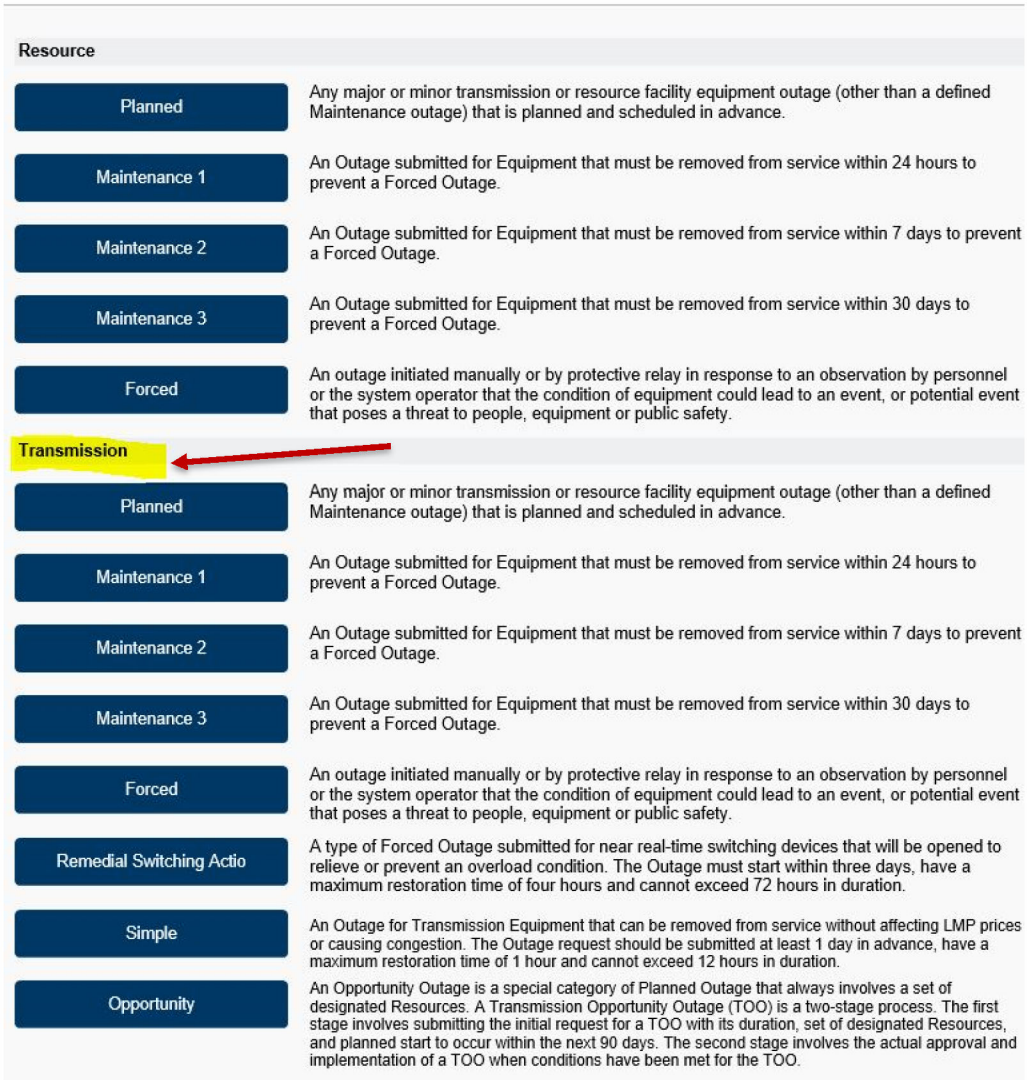


3.Clicking on the Outage Scheduler icon will open the Outage Scheduler. Click Create New Outage.

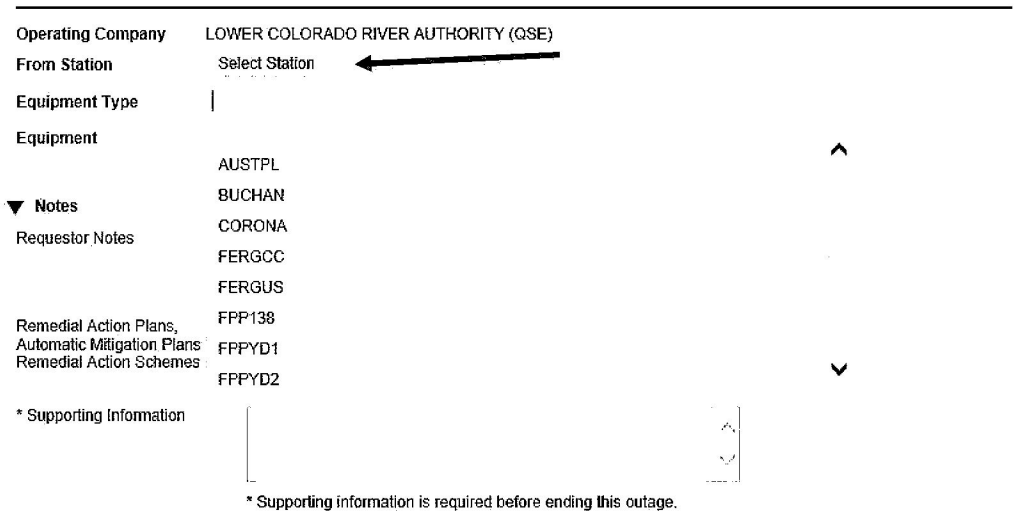


+	Wrn	ID	Category	Group Name	Station	To Station	Equip	Eq Type	Outage Type	Outage Status	Nature of Work	PI Start	PI End	Req Company	HSL	LSL	Nrml	Otg	Req Date	Vol	HIO	HIO > 90
		LCR00204531	Resource		GIDEON		GIDEONG2	UN	Planned	Canceled	Other	Mar 30 2020 06:00	Apr 20 2020 20:00	QLCRA	0	0			Jun 20 2019 16:35			
		LCR00216387	Transmission		JC_BAT		PSEUDO_BKR	CB	Unavoidable Ext	Accepted	New Equipment Energization	Feb 05 2020 00:00	May 04 2020 12:00	QLCRA			C	O	Dec 06 2019 10:28	12.0		
		LCR00216389	Transmission		JC_BAT		PSEUDO_SW1	DSC	Unavoidable Ext	Accepted	New Equipment Energization	Feb 05 2020 00:00	May 04 2020 12:00	QLCRA			C	O	Dec 06 2019 10:38	12.0		
		LCR00216390	Transmission		JC_BAT		WSL1	LD	Unavoidable Ext	Accepted	New Equipment Energization	Feb 05 2020 00:00	May 04 2020 12:00	QLCRA					Dec 06 2019 10:41	12.0		
		LCR00216391	Transmission		JC_BAT		PSEUDO_SW2	DSC	Unavoidable Ext	Accepted	New Equipment Energization	Feb 05 2020 00:00	May 04 2020 12:00	QLCRA			C	O	Dec 06 2019 10:42	12.0		
		LCR00217136	Resource		JC_BAT		JC_BAT_LD1	LR	Unavoidable Ext	Accepted	New Equipment Energization	Feb 14 2020 16:00	May 04 2020 12:00	QLCRA	0	0			Dec 20 2019 12:20			
		LCR00217137	Resource		JC_BAT		UNIT_1	UN	Unavoidable Ext	Accepted	New Equipment Energization	Feb 14 2020 16:00	May 04 2020 12:00	QLCRA	0	0			Dec 20 2019 12:22			

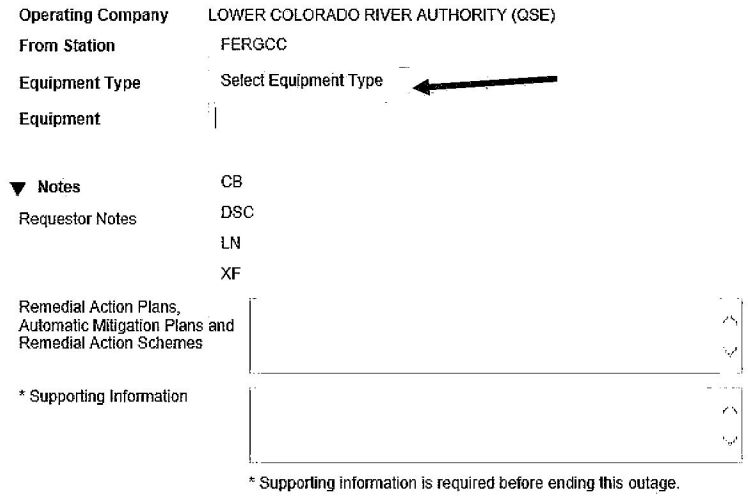
4.Select Transmission Outage and the appropriate level of outage that needs to be created (i.e. Planned, Forced, etc.)



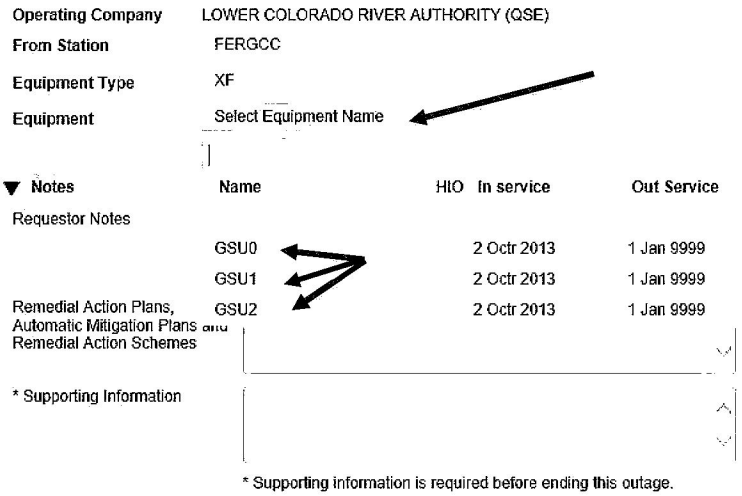
5.Fill in the required information just as you would if creating a Resource outage and then select the station name from the drop down menu.



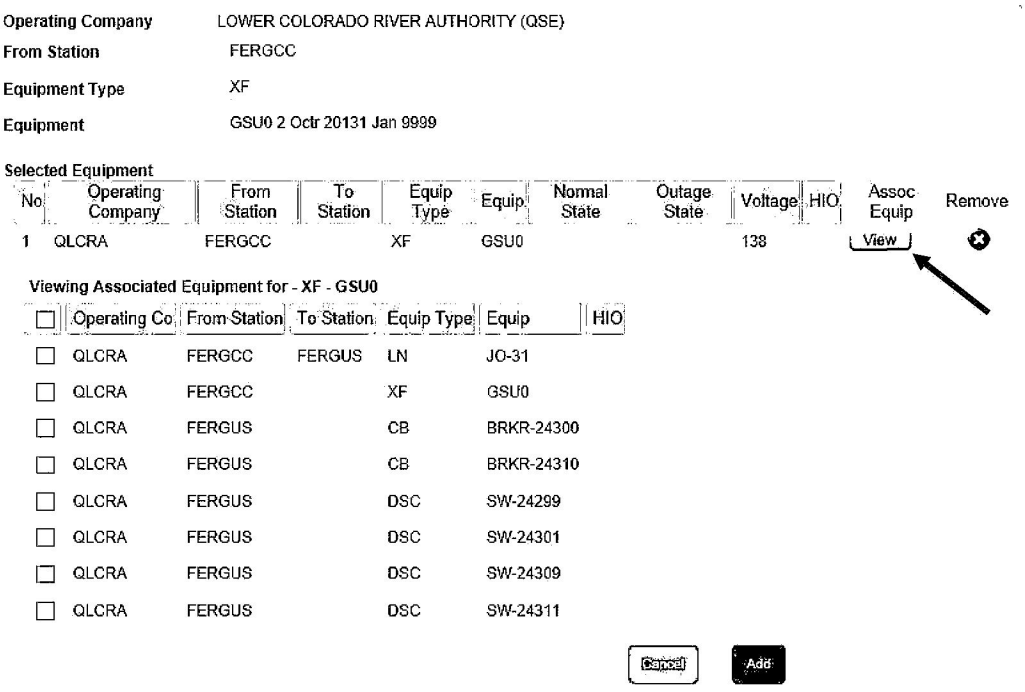
7.Once the station name is chosen, select the equipment type and select the type of equipment being placed into an outage. For example, select CB is circuit breakers need to be in outage or XF for transformers.



8.Once the equipment type is selected click in the field that says Equipment and you will be asked to select the actual Equipment Name for the outage. Click on the particular equipment to select it.



9.Some transmission elements have corresponding elements that must be placed in outage at the same time. Once an element has been selected, click the button that says View in the Assoc Equip column. This will show a list of all associated items that will need to be placed in an outage along with the item you selected. Simply select those elements to add them to the outage.



10.Once the associated elements have been added, fill in the Requestor's Notes and click the Submit button.

Hydro Control System

Working Copy - Disaster Recovery Plan

Version 2

Lower Colorado River Authority

Prepared By:

Lower Colorado River Authority

Hydro Control System

320 Buchanan Dr.

Buchanan Dam, TX 78609

[redacted]

Table of Contents

Section 1- Plan Approval

As the assigned designated authority for the Hydro Control System, I hereby certify that this disaster recovery plan is complete, and that the information contained within this plan provides an accurate representation of the application of the system and hardware, software and telecommunications components.

X

Ryan Schnitzler
Director, Dam and Hydro

Section 2- Plan Design

[redacted]

(a) Background

The following recovery plan objectives have been established:

[redacted]Disaster Recovery operations [redacted]

[redacted]

[redacted]

3. [redacted]
4. [redacted]

(b) Scope

This disaster recovery plan [redacted]. Procedures in this plan are designed to [redacted]. This plan [redacted]. This plan [redacted].

(c) Assumptions

The following assumptions were used when developing this plan:

1. [redacted]
2. Current backups of the system software, configurations, controller programs, [redacted]:

   a) [redacted]
   b) [redacted]
   c) [redacted]

3. [redacted]

a) [redacted]
b)

4. [redacted]
5. [redacted]

The Hydro Control System Disaster Recovery Plan does not apply to the following situations:

1. [redacted]
2. [redacted]
3. [redacted]

Section 3- Overview

This section [redacted]

(a) System Description

The information included provides [redacted]

1. [redacted]

[redacted]

[redacted]

[redacted]

2. **Physical Location** –

a) **Buchanan Dam (x 5731 /** [redacted] **)**– is the first upstream dam in a series of dams located along the Colorado River that are operated by LCRA. Buchanan dam [redacted].

b) **Inks Dam (x 5741 /** [redacted] **)**– is the second dam operated by LCRA. Inks dam [redacted].

c) **Wirtz Dam (x 5732 /** [redacted] **)** – is the third dam operated by LCRA. Wirtz dam [redacted].

d) **Starcke Dam (x 5742 /** [redacted] **)** – the fourth dam operated by LCRA. Starcke dam [redacted].

e) **Mansfield Dam (x 5743 /** [redacted] **)** – is the fifth dam operated by LCRA. Marshall Ford [redacted].

[redacted]

f) **Austin Dam (x 2707 / [redacted])**– is the sixth and last downstream dam in the series of dams operated by LCRA Hydro. Austin [redacted]

g) **ROCC (x 3041 / Redbud, [redacted])**– is the [redacted].

h) **HOCC (x 3041 / [redacted])** – [redacted] The HOCC [redacted].

i) **Buchanan Admin Building ([redacted])**– [redacted].

j) **Buchanan Weld Shop (Buchanan Dam)** – [redacted].

3. **Backup Procedure –** [redacted].

(b) Execution Strategy

1. [redacted].

   [redacted].

2. [redacted]

[redacted]

(c) Roles and Responsibilities

This plan establishes [redacted].

1. **Hydro Operations (x 3041/3042) –** [redacted]
2. **Hydro Maintenance (plant phones listed above)–** [redacted]
3. **Hydro Controls (x 3054) –** [redacted]
4. **Hydro Management (x 3047)–** [redacted]
5. **ISO (x** [redacted]
6. **IT Enterprise Network (x ####) –** [redacted]
7. **Hydro Cyber Security Coordinator (x 3054)–** [redacted]
8. **Telecom (TOC – 512-356-6450) –** [redacted]

Section 4- Activation and Notification

The Activation and Notification [redacted]. This phase [redacted].

(a) Activation Criteria and Procedure

[redacted]:

1. [redacted]
2. [redacted].

The following persons or roles may activate the plan if one or more if one or more of these criteria are met:

1. [redacted].

(b) Notification

[redacted]. Contact information for appropriate POCs is included [redacted]

For the [redacted] are used:

1. [redacted].
2. [redacted].
3. [redacted].
4. [redacted].

5. [redacted]

6. [redacted]

[redacted]

Section 5- Recovery

The [redacted]

(a) Recovery Procedures

The following procedures are provided for recovery of [redacted]

1. [redacted]

[redacted]

2. [redacted]

a) [redacted] (48 hr maximum remote operations recovery time) –

i) Scenario 1 – [redacted]

[redacted]

a. [redacted]

ii) Scenario 2 - [redacted]

a. [redacted]

b) [redacted] –

i) Scenario 1 – [redacted]

a. [redacted]

ii) Scenario 2 - [redacted]

a. [redacted]

3. [redacted]

[redacted]

[redacted]

[redacted]

b) [redacted]

[redacted]

vii) [redacted].

c) [redacted]

[redacted]

[redacted].

iv) [redacted]

[redacted]

b. [redacted].
c. [redacted].

v) [redacted].

vi) [redacted]

vii) [redacted]

[redacted]

[redacted]

e) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

(b) Event Documentation

All recovery events, including actions taken and problems encountered during the recovery and reconstitution effort shall be well-documented, [redacted]. It is the responsibility of each team or person to document their actions during the recovery effort, and to provide that documentation to the Plan Coordinator.

Include the following information in documentation of recovery effort:

[redacted]

4. [redacted]

[redacted]

[redacted]. Notification of this declaration will be provided to all business and technical POCs.

(c) Deactivation

Section 6- APPENDIX

(a) Appendix A Test and Maintenance Schedule

This plan shall be reviewed and tested on an annual basis. [redacted]

[redacted]

(b) Appendix B Vendor Contact Information

[redacted]

Section 7- Revision History

Revision Number	Revision Date	Description	Editor
1	02-4-2014	Initial issue finalized	Ryan Schnitzler
2	01-06-2016	Updated plan for new system design. [redacted]".	Ryan Schnitzler
3	08/01/2018	Updated plan for [redacted].	Brenard Butler
4	07/29/2019	Updated plan for [redacted].	Brenard Butler
5	01/14/2020	Updated contact numbers for **Hydro Controls, Mangement,** and **Cyber Security Coordinator**	Brenard Butler
6	02/08/2021	Updated contact numbers for **Hydro Controls** and **Cyber Security Coordinator**	Brenard Butler

§25.53 (e)(2)(D) A pandemic and epidemic annex

Refer to Bates Pages: 66-72

§25.53 (e)(2)(F) A cyber security annex

Lower Colorado River Authority

Security and Risk

(Physical Security, Cybersecurity and Risk Management)

Procedures Manual

1158

Table of Contents

EFFECTIVE: Jan. 2, 2018. Amended March 13, 2018; Aug. 2, 2019; and Oct. 30, 2019.

Physical Security

This procedure establishes physical security requirements and worker responsibilities for LCRA facilities and properties.

Terms and Definitions: The following terms and definitions are used throughout this document.

- **Access badge** – An electronic credential card used to gain physical access to an area.
- **General access** – An area to which access is controlled but available to all workers.
- **Physical security systems** – Software and hardware used to provide physical security, including security cameras, video recorders, access badge readers, burglar and duress alarm systems, security sensors, electrified lock sets, intrusion detection systems, and associated information technology hardware and software.
- **Restricted area** – An area to which access is strictly controlled and requires special approval to have access.
- **Regulated area** – A restricted area to which access is governed by a regulatory standard or law.

General Security Requirements

Duty to Report: Workers have a duty to report suspected criminal activity involving LCRA facilities, property and workers, as well as any violations of the physical security procedures.

Criminal activity and security emergencies shall be reported promptly to Public Safety Dispatch at ext. 8911, or 512-730-8911 from an external phone. Procedure violations shall be reported to Public Safety, Human Resources at 512-473-4004, a direct supervisor or the ethics hotline at 877-820-0535.

Official Identification Cards: Public Safety may issue official identification cards to support the business needs of the organization. All LCRA identification cards remain the property of LCRA, and they must be returned upon request. Identification cards only shall be used for their intended purposes. Lost or stolen identification cards shall be reported to Public Safety.

Protection of Issued Equipment and Property: Workers are responsible for LCRA equipment and property issued to them. Reasonable precautions shall be taken to prevent the loss, theft, destruction or unauthorized use of LCRA equipment and property. Property theft shall be reported to Public Safety Dispatch as soon as the theft is discovered. Lost property shall be reported to the worker's immediate supervisor.

Awareness Training: Employees will receive initial security awareness training, which includes information on how to report emergencies, appropriate access badge use and general workplace security information. Additional training may be required for workers with physical access to regulated or restricted areas.

Threat Response Level: The chief of Public Safety shall determine the threat response level for the organization and establish the appropriate level of protective measures.

Exceptions: Exceptions to the Physical Security procedures may be granted for justified business needs. Requests shall be made in writing and approved by the chief of Public Safety. Requests for exceptions will be reviewed at least annually.

Physical Access

Physical access shall be managed to provide workers the necessary access to perform their duties while still limiting unauthorized access.

Access Badges: Public Safety will issue an access badge to each worker requiring physical access to LCRA facilities after Human Resources assigns an employee identification number to the worker and any appropriate background checks have been completed.

Workers are responsible for their issued access badges and will be held accountable for their use. Access badges are not to be shared or used by anyone other than the worker to whom they are assigned. Workers shall immediately report lost and stolen access badges to Public Safety Dispatch at ext. 6322. Workers may be charged a fee to replace missing access badges.

Access badges shall be displayed at or above waist level on the outermost layer of clothing. This does not apply to industrial environments if it creates a safety hazard.

Workers shall not attach anything to the access badge that may identify it with LCRA. This helps limit the possibility of unauthorized use if the badge is lost or stolen.

Temporary Access Badges: Temporary access badges are available at some locations for short-term use when workers forget their assigned access badges. Temporary access badges cannot be programmed for entering restricted areas.

Temporary access badges must be returned at the end of the borrowing worker's shift. Any unreturned temporary access badges will be suspended, along with the borrowing worker's assigned access badge. The worker's assigned access badge will be reactivated after the temporary access badge is returned or the replacement fee is paid.

Use of Access Badges: Workers are expected to use individually assigned access badges in accordance with this procedure. Inappropriate use of access badges is prohibited.

LCRA management exclusively determines what is appropriate or inappropriate badge use. Although not an all-inclusive list, inappropriate use may include the following:

- Using or allowing someone to use an access badge that is not assigned to that person.
- Piggybacking or tailgating through a door or gate into a secure area.
- Lending a badge to another person.
- Using an access badge in excess of one's authority.
- Cloning or copying an access badge.

Use of PIN and Access Codes: Workers are responsible for the proper control and use of codes in areas where personal identification numbers (PINs) and access codes are used to gain access or activate/deactivate physical security systems. Codes must be kept secure and may not be shared with unauthorized people. Individually assigned codes are preferred, and they shall be changed if there is reason to believe unauthorized people have learned the codes or when workers with knowledge of the codes no longer require access. Shared codes may be provided for certain uses, and they shall be changed at least quarterly.

Codes must be numbers generally unknown and difficult to guess. Codes may not match the worker's employee identification number or be simple or repeating numbers (such as: 1234, 0000, 1111, 9876, etc.).

Statutory and Regulatory Requirements: LCRA complies with numerous physical security statutory and regulatory requirements, including many focused on specific areas and work sites. All workers entering such locations also will comply with any additional policies and procedures to meet those requirements.

Physical Access Requests: All workers will be provided general access. Requests for access to restricted and regulated areas must be made using the appropriate form. Access will not be provided until all approvals are received.

Access shall be based on least privilege – granting each worker the minimum level of access needed to perform their work functions.

Access removal will be in accordance with the LCRA Employee Policy Manual. Workers who receive a request to terminate system and/or facility access for anyone shall immediately contact Human Resources to ensure the access removal process has been initiated.

Physical Access Reviews: Access lists for restricted and regulated areas will be reviewed at least annually by an authorized approver for each area. Some regulated areas may require more frequent reviews as determined by site-specific security policies.

Visitors

Visitors will be managed properly to maintain appropriate security, including the requirement to escort visitors in areas not normally open to the public. Visitors will be documented and managed in accordance with the procedure.

Visitors Logs: Public Safety will work with facility managers to determine where visitor logs are appropriate based on security risk. For sites with visitor logs, all visitors will be logged to include the visitor's name, escort name, reason for visit, and the date and time of arrival and departure. Visitors will be escorted while in restricted areas.

Each site will have a designated employee responsible for maintaining and reviewing visitor logs. Completed visitor logs will be forwarded to Public Safety monthly for records retention.

Visitor and Contractor Risk Assessments: Visitors, including contractors, requiring access to certain restricted sites are required to provide valid identification, and they will have a risk assessment performed by Public Safety as a condition of entry. In addition to verifying the person's identity, Public Safety will conduct a risk assessment to determine if allowing access creates an excessive security risk. Visitors may be denied access at the discretion of Public Safety without providing the cause for rejection. Public Safety will attempt to notify the LCRA sponsor if a visitor will be denied entry. Contractors receiving security access badges must adhere to this procedure as applicable.

Results from risk assessments are generally confidential. Due to legal restrictions, some causes for rejection may not be shared with the visitor or the LCRA sponsor.

Restricted areas requiring a risk assessment include power plants, dams, control centers, Public Safety offices, Hilbig Gas Storage Facility and other areas as determined by management.

Visitor risk assessments generally are requested by contacting the security officer at the facility being visited. If security is not stationed at the facility, contact Public Safety Dispatch at ext. 6322 for guidance. Risk assessments on foreign nationals should be requested at least three business days prior to arrival.

Identification Requirements: Each visitor and contractor subject to a risk assessment must provide one of the following forms of acceptable identification:

- Driver's license or identification card issued by a state or territory of the United States.
- United States passport or passport card.
- United States military identification or Common Access Card.
- United States Department of State Personal Identification Card.
- United States Permanent Resident Card (Form I-551).
- United States Employment Authorization Card (Form I-766).

- United States B1/B2 visa and Border Crossing Card.
- Foreign passport with a valid United States visa or dated entry mark.

LCRA will not accept any other form of identification, including these common documents:

- Social Security card.
- Birth certificate.
- Foreign government consular identification card.
- Foreign passport without a valid United States visa or dated entry mark.
- Foreign government driver's license or identification card.
- International driver's license.
- United States Transportation Worker Identification Credential (TWIC) card.
- School, university or employer identification card.

Physical Security Systems

Physical security systems should be designed, deployed, protected and managed to meet the needs of the organization and remain compliant with regulatory requirements and best practices. Workers are accountable for properly using physical security systems.

Physical Security Systems Management: Physical security systems are considered enterprise assets and are managed by Public Safety. Public Safety is responsible for all maintenance and modifications to physical security systems. Workers shall not disable, tamper with or make changes to physical security systems without prior approval.

Physical Security Systems Standards: Public Safety will establish standards for all physical security systems. Public Safety will ensure systems connected to LCRA networks are coordinated with the network administrators. Nonstandard systems and components may be authorized on a case-by-case basis when a business need cannot be met using standardized equipment. The installation of unauthorized and "rogue" physical security systems is strictly prohibited.

Security Assessments: Public Safety will perform risk-based security assessments on LCRA properties to make physical security recommendations. Assessments will be performed periodically to evaluate the physical security needs of LCRA properties. Assessments also will be performed for all new installations or any time a significant change is requested. The scope of the assessment will be determined on a case-by-case basis. Copies of the assessments will be provided to the facility manager but are protected from public disclosure. The facility manager shall provide a response to each recommendation using the form provided within the assessment document.

Physical Security System Data: Reports, video and other data from physical security systems may be used only for official business purposes. Requests for information should be made in writing using the approved request form available through Public

Safety. Information for criminal investigations will be turned over to LCRA Rangers or an appropriate law enforcement agency. Information for internal employee investigations shall be approved by Human Resources before the information is released.

Physical Security Monitoring: Public Safety Dispatch is the primary group responsible for monitoring physical security systems. All physical security systems will be made available to Public Safety Dispatch. Other work groups may be provided access to monitor physical security systems to assist in the performance of their respective operations. During a security event or public safety emergency, Public Safety will have primary control and operation of physical security systems.

Confidentiality of Security Systems Information: Information about physical security systems is considered confidential and shall be handled as such, including information on system design, specifications, monitoring practices and system-generated reports. This information shall not be released outside of LCRA without prior approval from the Legal department and Public Safety.

Emergency Situations

LCRA also has Public Safety and Environmental departments that help prevent emergencies and respond to emergencies when they occur. LCRA employees managing contractors, visitors or outside resources are responsible for ensuring those personnel are aware of the basic safety and notification policies for the facilities where they work.

Workers should not respond to an emergency if they are not trained and designated to respond. They should instead go to a safe location and contact the appropriate personnel. Employees should follow the notification procedures for their work locations or departments. Workers unsure of their facility's emergency notification procedures should contact the Public Safety Communications Center (LCRA Dispatch) by dialing 8-9-1-1 from an LCRA phone, or toll free from any phone at 866-527-2267. Anyone performing work at an LCRA work site is expected to review and understand the emergency plans for his or her work location.

Reporting Requirements: Reporting information in a timely manner can prevent situations from occurring or worsening. Workers must notify the appropriate group or person of emergencies or developing situations that:

- Could have a substantial impact on the ability to deliver services.
- Could have a substantial impact on quality of life, the public or the environment.
- Involve a serious on-duty injury or the death of an LCRA worker, contractor or visitor.
- Involve suspicious activity, crime, sabotage or other security concerns.

The appropriate person to contact varies by LCRA facility. Some LCRA facilities, especially power plants, have their own control centers. Employees at power plants

should contact the plant's control center first. Control center personnel will notify LCRA's Dispatch. Employees at locations other than power plants should call LCRA Dispatch by dialing 8-9-1-1 from any LCRA phone or toll-free at 866-527-2267 from any phone.

Employees consistently reporting incidents helps Public Safety identify trends and potentially escalating events early enough to effectively prioritize and manage critical resources. Dispatch will request emergency services and notify appropriate response staff and leadership in any situation that is growing or has the potential to affect the organization. Employees should contact LCRA Public Safety Dispatch or their facility's control center to report incidents if they are unsure of the notification process at their facility.

When workers report information to LCRA Dispatch or a control center, they should include the following information:

1. Their name and callback number.
2. The exact location of the emergency.
3. The nature of the emergency.
4. Potential impact to LCRA operations, if known.
5. What the caller plans to do.

Radio Communications: In the event of an emergency, workers should use whatever communications device is the most expedient. [redacted].

LCRA [redacted].

1. [redacted].
2. [redacted].

Cybersecurity

Cybersecurity Standards and Controls

LCRA Cybersecurity Framework: The Cybersecurity department is responsible for establishing cybersecurity standards and controls for all of LCRA. [redacted].

System Classification: A[redacted].

- [redacted].
- [redacted].

Authority of Cybersecurity Department: The LCRA Employee Policy Manual states the "Cybersecurity department's authority encompasses all LCRA information systems, [redacted] and associated information, regardless of form." The chief information security officer determines the content of the LCRA Cybersecurity Framework.

LCRA Cybersecurity Framework Implementation: The LCRA Cybersecurity Framework is developed with the input of system owners and other stakeholders. The framework's controls reflect the authoritative standards to which LCRA's business units and departments adhere. These authoritative standards will be reviewed on an annual basis by system owners to determine if there have been any changes to the standards that require a modification to the LCRA Cybersecurity Framework.

The Cybersecurity department provides security assessments, consultations and other services to assist stakeholders with understanding and implementing cybersecurity controls. [redacted]. In such instances, s[redacted]. In some instances, [redacted].

Use of Non-LCRA Issued Devices

Workers may use non-LCRA-issued devices, such as personal computers, smart phones, etc., to connect to LCRA resources remotely or while on LCRA premises as long as the following security precautions are met:

Connecting to LCRA Resources: Workers may retrieve email and other information on their personal devices such as smartphones provided that:

- [redacted].
- [redacted].
- [redacted].
- [redacted].
- [redacted].

Use of LCRA Wireless Networks: Personally owned devices may only connect to LCRA Wi-Fi networks specifically designated for such use. Personally owned devices may not use any other wired or wireless network.

Portable Media: Only LCRA-issued USB drives should be used on LCRA systems or to store LCRA information. If a USB drive is required for an employee's job duties, he or she should request one through the Service Desk. [redacted]. Please call the Service Desk at ext. 3300 [redacted]. Generic flash drives such as those given away at trade shows should not be accepted or used.

Other Personally Owned Devices: Personally owned devices, such as USB drives, hard drives, etc., may not be attached to LCRA network equipment or computers at any time. Computer ports may not be used to charge personal devices.

Information Protection

Confidential or privileged information, as defined in the LCRA Employee Policy Manual, must be stored only using devices, network locations and cloud-storage providers that are approved by the Cybersecurity department. Contact Digital Services for additional information regarding approved storage methods. Confidential or privileged information also must be adequately secured during transfer such as when being emailed, uploaded, etc.

Securing Media:

- Workers must ensure only individuals with an authorized business need have access to digital and nondigital media containing sensitive data.
- Workers must ensure digital and nondigital media containing sensitive data is used only on authorized systems.
- Media containing sensitive information must be secured in areas that are not publically accessible.
- Media must be secured while being moved between controlled areas. Workers must maintain possession of the media/documents at all times.
- Media protections remain in force until the media is properly destroyed by shredding or other approved sanitization method. Contact Digital Services for assistance in securely destroying digital information.
- Workers shall take reasonable precautions to prevent loss, theft or unintended destruction of digital and nondigital media. Workers are responsible for reporting loss, theft or destruction of such media to the Service Desk immediately upon discovery.

Digital Information Storage: LCRA digital information must be stored on Cybersecurity department-approved locations configured with security controls adequate for the type of information being housed.

- Approval is required for all media types, including:
    - Cloud storage locations.
    - Infrastructure (server-based) locations.
    - Portable media.
- Official electronic copies of documents must not be stored on laptop or desktop computers. Instead, they should be stored on corporate servers (such as designated SharePoint sites) so that files are backed up and properly secured.

Digital Information Transfer: When files must be shared outside of LCRA, the following security controls must be used:

- When emailing files to an outside source, the documents must be sent using a Cybersecurity department-approved encryption method.
    - Compression utilities, such as 7-Zip, have encryption methods available.
    - Passwords must never be sent in the same email as the file.

- If sharing files using an approved cloud provider, the files must be encrypted prior to storing them on that location.
- When available, encrypted communication channels must be employed (HTTPS, SFTP, etc.)
- Never use personal devices to store or transport LCRA information. Contact Digital Services for an approved storage device if there is a justified business need.

Information Disclosure: Workers should not disclose information to outside sources unless they are explicitly authorized to do so. If you are not sure if you are authorized, presume you are not.

Privacy

Workers should not have expectations of privacy in the use of LCRA email, computer systems, voice mail, pagers, cellular telephones, tablets and mobile radios. LCRA may inspect, use, or disclose any electronic communications and data without notice. Use good judgment in the tone and content of electronic communications, and do not communicate or state anything that could damage the reputation of or otherwise harm LCRA or its workers if made public.

Monitoring: LCRA technology and systems are for the use of authorized users only. Workers are subject to having all of their activity on LCRA systems monitored and recorded by systems personnel. Anyone using these systems expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, systems personnel may provide the evidence of such monitoring to law enforcement officials.

Software Installation and Use

All computer software used on an LCRA computer shall be licensed for use by LCRA. Any software found on an LCRA computer and determined not to have been licensed by LCRA will be removed.

Approved Software: Contact the Service Desk to have LCRA-approved and LCRA-licensed software installed on LCRA computers.

- LCRA software is not for use on non-LCRA computers.

Unapproved Software: Unapproved software for which there is a business need must have an approved exception request on file before the software is installed.

- Submit the exception using ServiceNow.
- If the software is approved, the Service Desk will arrange to install the software.

Security Requirements

LCRA workers must adhere to the following additional requirements to help protect our computers and systems from malicious actors.

Credentials Protection:

- Workers must never share their accounts or passwords with anyone else.
- Passwords for LCRA accounts must be unique. Never use an LCRA password on another system.
- Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames. Workers may not store passwords in Word documents or Excel files, on SharePoint sites or in any other format or location on LCRA systems. Electronic storage of passwords is authorized only on designated systems approved by Cybersecurity.
- If a worker has more than one account, such as a regular account and an administrative account, the passwords must be different.
- When changing passwords, make the new password significantly different from the current one; i.e., do not simply increment a number or use another predictable pattern.

Defeating Controls: Workers must never attempt to defeat security controls, such as disabling workstation antimalware or firewalls, without authorization. Workers must never attempt to grant themselves increased privileges to a system, i.e., trying to obtain administrator or other rights without authorization.

Least Privilege: Workers only should have access to those systems and data necessary to perform their job functions. Accessing data for which there is not a legitimate business need is a violation of the concept of least privilege and could result in disciplinary action.

Suspicious Behavior: If an LCRA worker notices his or her computer behaving in an unexpected way that may indicate a compromise, he or she should report this to the Service Desk for further analysis. Additionally, suspicious behavior observed of another person should be reported to Public Safety.

Violations

Workers who violate or intentionally circumvent LCRA's cybersecurity policies, controls or requirements may be subject to disciplinary actions.

Risk Management

LCRA will maintain a comprehensive risk management program that identifies, assesses, monitors and manages material risks to LCRA's mission and objectives. LCRA will pursue operational excellence and accept normal business risks while complying with all applicable laws and regulations, protecting the environment under its stewardship, and preserving its reputation.

Multiple risk management functions and activities are in place across LCRA, which serve to:

- Manage financial, market and business risks to ensure the financial integrity of LCRA;
- Manage, develop, use and protect LCRA assets to provide reliable, cost-effective services for its customers; and
- Manage LCRA operations in a manner to reduce or mitigate, to the extent feasible, the conditions, hazards and practices that may cause losses.

Insurance

The insurance program provides services to manage incidents where damages to people or property cause or may cause a potential financial loss to the agency. Employees should immediately report all incidents to their supervisors and/or managers and enter them into the safety incident management tool.

- **Vehicle Incident:** In the event of a vehicle incident, all workers shall adhere to the Fleet Operators Procedure Manual section on Accidents, After-Hours Emergencies and Roadside Assistance, and report the incident to his or her supervisor and/or manager immediately.
- **Property Damage:** In the event natural and man-made exposures occur resulting in physical damage to LCRA's property and/or a third party, the worker is responsible of reporting damages to his or her supervisor and/or manager immediately. All property damage claims will be processed by the Risk and Business Continuity department.
- **Workers' Compensation:** In the event a worker is injured on the job, the worker is responsible for immediately reporting the incident causing the injury to his or her supervisor and/or manager. Employees are to work directly with Human Resources to ensure the proper treatment and processing of required claims.
- **General Liability:** If a worker witnesses a nonworker incident on LCRA property, the worker is responsible for immediately reporting the incident to his or her supervisor and/or manager and for entering the incident into the safety incident management tool as soon as possible.

Business Continuity Program

The Risk and Business Continuity team is responsible for governance and oversight of LCRA's emergency operations and business continuity planning activities. All mission-critical facilities, operations and technology are required to have the appropriate plans in place to ensure approved strategies are documented in actionable plans for responding to interruption risks.

Business continuity management plans are defined as:

- **Facility Emergency Operations Plan (FEOP):** [redacted]
- **Business Continuity Plan (BCP):** [redacted].
- **Disaster Recovery Plan (DRP):** [redacted].
- **Information System Contingency Plan (ISCP):** [redacted].

§25.53 (e)(2)(G) A physical security incident annex

Refer to Bates Pages: 93-105, 1158-1166