

**NERC Project**  
**Central Repository**  
**for Security Event, Curtailment and Interruption Information**

**in**  
**Partial Fulfillment**  
**of**

**– FERC Order 605 –**

**Phase I**  
**Announcement Briefing**

**February 28, 2001**

**By**

**Central Repository Task Force (CRTF)**  
**And**  
**NERC Staff**

## Table of Contents

Introduction. Project Description.....	3
Phase I - March 1, 2001.....	3
SECTION 1. Adoption of Value-Added Template with S&CP-Style CSV File for Security Event Input to OASIS .....	4
1.1 Provider Posting of Security Events.....	4
1.2 Template: securitypost.....	4
SECTION 2. Mapping IDC TLR Excerpts to OASIS Security Event Template Items .....	6
2.1 IDC Database TLR Status Message Data Elements.....	6
2.2 Book of Flowgates Additional Fields Considered for OASIS Security Event Template Requirements.....	6
2.3 Recommended Mapping - TLR Message to SecurityPost Template .....	7
2.3.0 The TLR Event-Recognition Procedure.....	7
2.3.1 Event ID.....	8
2.3.2 Security_Type.....	8
2.3.2 Initiating_Party.....	8
2.3.4 Responsible_Party.....	8
2.3.5 Procedure_Name.....	8
2.3.6 Procedure_Level.....	8
2.3.7 Facility_Class.....	8
2.3.8 Facility_Limit_Type.....	8
2.3.9 Facility_Location.....	8
2.3.10 Facility_Name.....	9
2.3.11 Start_Time.....	9
2.4 Additional Information to be Posted in the NERC TLR Logs .....	9
SECTION 3. Mapping WSCC USF Excerpts to OASIS Security Event Template Items .....	10
3.1 WSCC USF Email Message Data Elements.....	10
3.2 Recommended Mapping - USF Message to SecurityPost Template.....	11
3.2.0 The USF Reduction Event-Recognition Procedure.....	11
3.2.1 Event ID.....	11
3.2.2 Security_Type.....	11
3.2.2 Initiating_Party.....	11
3.2.4 Responsible_Party.....	11
3.2.5 Procedure_Name.....	11
3.2.6 Procedure_Level.....	11
3.2.7 Facility_Class.....	11
3.2.8 Facility_Limit_Type.....	11
3.2.9 Facility_Location.....	12
3.2.10 Facility_Name.....	12
3.2.11 Start_Time.....	12
SECTION 4. A Database Schema for Security Events Built from IDC TLR Status and USF Action Step Messages.....	13
4.1 Existing NERC IDC TLR Status Message Table in the Central Repository Database.....	13
4.2 Proposed WSCC USF Reduction Message Tables in the Central Repository Database.....	13
4.3 Proposed Security Event Tables in the Central Repository Database.....	14
4.4 Attributes of Security Event and Security Step Tables in the Central Repository Database.....	16
SECTION 5. Security Events Distribution – NERC Web-based Application.....	17
5.1 Site for Polling and Pull-based Applications.....	17
5.1.1 NERC TLR Example.....	17
5.1.2 WSCC USF Example.....	18
5.2 OASIS S&CP security Template at NERC CRC – for Polling and Pull-based Applications.....	19
5.2.1 URL String.....	<b>Error! Bookmark not defined.</b>
5.3 Call-Level Interface Programmatic API for Polling and Pull-based Applications.....	19
5.4 SECURITYPOST TMP Message with TP Forwarding URL -- Push-based Application.....	19
5.5 SECURITYPOST Direct CSV Upload at TP Forwarding URL -- Push-based Application.....	20
SECTION 6. TP Tag Forwarding for Adjustments to be Sent to OASIS Nodes to Supply security and scheduledetail Templates .....	21
6.1 ADJUST Message Modifications.....	23
6.2 The CURTAIL_POST Message or curtailpost template CSV Upload.....	24
6.2.1 Usage.....	24

## Introduction. Project Description

The Central Repository will provide a single, independent, consolidated source for the storage and retrieval of historical data including:

- ?? Security Events
- ?? Curtailment Logs
- ?? Interruption Logs
- ?? Outage Information
- ?? E-tags
- ?? Schedules

Necessary components include hardware, software, communications hardware, and a communications network. The capabilities of the Central Repository will allow for any NERC certified entity to view, query, or download any or all of the databases for desired information. The Central Repository will receive data constantly and that data will be accessible to entities within seconds of data being received by the system.

The Central Repository for Security Event, Curtailment and Interruption Information will act as a conduit for information which transmission providers are required by FERC to provide on OASIS. The data will be provided automatically from the NERC Interchange Distribution Calculator (IDC) for the Eastern Interconnection and from the WSCC Unscheduled Flow (USF) reduction procedure email system for the Western Interconnection. No data collection is currently contemplated for the ERCOT Interconnection. The Repository must be made available by March 1, 2001 in accordance with the FERC Order 605, Docket No. RM98-3-000, May 27, 2000, "Open Access Same-time Information System Final Rule"

The CRCII Project will be accomplished in conjunction with the planned NERC Transaction Information System Cache (TISCache) Project, a central repository for all tagging information. This will require a phased approach for CRCII:

### ***Phase I - March 1, 2001***

Due to the time constraint imposed by FERC Order 605 requiring Repository to be operation by March 1, 2001, the CRCII will be initially implemented at the NERC office using existing telecommunications and computer hardware. This Phase of the project will consist of the following tasks:

1. IDC Changes — Automation of the NERC Transmission Loading Relief (TLR) Logs for the Eastern Interconnection — have the IDC automatically generate TLR Log information and forward it to the Central Repository.
2. NERC TLR Log Changes — Modify the format of the TLR Logs to conform to the required data format of the Central Repository.
3. WSCC USF Changes — Modify the WSCC USF reduction procedure messaging system to generate the required data format of the Central Repository.
4. E-Tag Changes — Modify the E-Tag messages generated by the tag authorities to include TMP messages to OASIS Nodes as requested.
5. Master Registry Changes — Modify the Master Registry to include an optional TP forwarding URL for OASIS Nodes to allow forwarding of curtailment (adjustment) information.
6. OASIS S&CP Changes — Modify the OASIS S&CP to correct the data definition for the OASIS Curtailment and Interruption Information Templates to conform to the CRCII requirements.
7. CRCII Software Development — Develop necessary software to support display, query and audit capabilities for the Central Repository.
8. Communications and Computer Hardware Changes — Make any necessary changes to the communications and computer hardware at the NERC office to accommodate Phase I CRCII requirements.

# PHASE I – SECURITY EVENTS

## SECTION 1. Adoption of Value-Added Template with S&CP-Style CSV File for Security Event Input to OASIS

This is a proposal to publish an additional non-S&CP documented template to include the CSV format for input of security event information on OASIS. By publishing a standard template for the input, NERC’s Central Repository will be able to provide the security event information to OASIS that is generated from Eastern Interconnection TLR events as delivered from the IDC. Also with a standard template, WSCC will be able to provide similar security data from the Western Interconnection for OASIS to be distributed from the Central Repository. ERCOT security events and local transmission relief events may also use the input template for other security events on OASIS. The OSC is the only group that might standardize this value-added template to be used by the industry. Its format is recommended as follows:

### 1.1 Provider Posting of Security Events

Provider Security Event Posting (INPUT) (*securitypost*) may be used by the Transmission Provider (TP) to post security events affecting the actual security of transmission that has been scheduled for energy exchange. Primary\_Provider\_Code and Primary\_Provider\_Duns shall be determined from the registered connection used to input the data.

### 1.2 Template: securitypost

1. **Input**

EVENT_ID	(NERC TLR or USF ID No.)	(0{Alphanumeric}25 => Optional)
SECURITY_TYPE	(L for "LIMIT" or O for "OUTAGE")	(1{Alphanumeric} => Required)
INITIATING_PARTY	(e.g., CA/TP code)	(0{Alphanumeric}4 => Optional)
RESPONSIBLE_PARTY	(e.g., SC code)	(1{Alphanumeric}25 => Required)
PROCEDURE_NAME	(e.g., "TLR", or registered)	(0{Alphanumeric}25 => Optional)
PROCEDURE_LEVEL	(dependent on PROCEDURE_NAME)	(1{Alphanumeric}25 => Required)
FACILITY_CLASS	(e.g., "FLOWGATE", "LINE", etc.)	(0{Alphanumeric}25 => Optional)
FACILITY_LIMIT_TYPE	(e.g., "THERMAL", "STABILITY", etc.)	(0{Alphanumeric}25 => Optional)
FACILITY_LOCATION	("INTERNAL" or "EXTERNAL")	(0{Alphanumeric}8 => Optional)
FACILITY_NAME	(e.g., path or flowgate name)	(0{Alphanumeric}25 => Optional)
START_TIME		(16{Alphanumeric}16 => Required)
  
2. **Response (Acknowledgment)**

SECURITY_REF	(OASIS-Generated ID)	(1{Alphanumeric}10 => Required)
EVENT_ID		
SECURITY_TYPE		
INITIATING_PARTY		
RESPONSIBLE_PARTY		
PROCEDURE_NAME		
PROCEDURE_LEVEL		
FACILITY_CLASS		
FACILITY_LIMIT_TYPE		
FACILITY_LOCATION		
FACILITY_NAME		
START_TIME		
TIME_OF_LAST_UPDATE		
  
3. **CSV Upload**

```
VERSION=nn.n
TEMPLATE=securitypost
OUTPUT_FORMAT=DATA
PRIMARY_PROVIDER_CODE=aaaa
PRIMARY_PROVIDER_DUNS=nnnnnnnnn
RETURN_TZ=aa
DATA_ROWS=nnn
COLUMN_HEADERS = "EVENT_ID", "SECURITY_TYPE", "INITIATING_PARTY",
                  "RESPONSIBLE_PARTY", "PROCEDURE_NAME", "PROCEDURE_LEVEL",
                  "FACILITY_CLASS", "FACILITY_LIMIT_TYPE", "FACILITY_LOCATION",
                  "FACILITY_NAME", "START_TIME"
[nnn rows of comma separated fields corresponding to COLUMN_HEADERS.]
```

## 1. CSV Response

REQUEST\_STATUS = *nnn*  
ERROR\_MESSAGE=*aaa*  
TIME\_STAMP = *yyyymmddhhmmsstz*  
VERSION=*m.n*  
TEMPLATE=*securitypost*  
OUTPUT\_FORMAT=DATA  
PRIMARY\_PROVIDER\_CODE=*aaaa*  
PRIMARY\_PROVIDER\_DUNS=*nnnnnnnn*  
RETURN\_TZ=*aa*  
DATA\_ROWS=*nnn*  
COLUMN\_HEADERS = "SECURITY\_REF", "EVENT\_ID", "SECURITY\_TYPE", "INITIATING\_PARTY",  
"RESPONSIBLE\_PARTY", "PROCEDURE\_NAME", "PROCEDURE\_LEVEL",  
"FACILITY\_CLASS", "FACILITY\_LIMIT\_TYPE", "FACILITY\_LOCATION",  
"FACILITY\_NAME", "START\_TIME", "TIME\_OF\_LAST\_UPDATE"

[*nnn* rows of comma separated fields corresponding to COLUMN\_HEADERS. With the exception of the addition of SECURITY\_REF and TIME\_OF\_LAST\_UPDATE, this is an echo of the input data.]

## SECTION 2. Mapping IDC TLR Excerpts to OASIS Security Event Template Items

This section develops the mapping of IDC information to OASIS information. Currently IDC is sending to the NERC TLR Status Web Site Database the security event information that is sufficient for the OASIS security template in complying with FERC Order 605. The IDC is the only system that can supply the NERC TLR Status Web Site Database with data generated by NERC's TLR Procedure for the Eastern Interconnection (Policy 9, Appendix 9C1). The current method makes use of a push-based delivery mode to the NERC TLR Status Web Site Database, using a call-level interface.

### 2.1 IDC Database TLR Status Message Data Elements

The following active, current, TLR information is sent as excerpts from the IDC to the NERC TLR Web Site for each event and associated Level (Status) changes:

<b>IDC TLR Message to NERC</b>		
<b>Record_ID</b> – OATI generated		
<b>Recipient</b> – A query of SCIS database for a list of all members		
<b>Beep</b> – Not used		
<b>CA</b> – The CA side of the flowgate that's causing the constraint. Also the initiating CA calling the SC for relief.		
<b>SC</b> – Responsible party. The SC in whose Control Area the TLR is issued.		
<b>Sender</b> – SC code (IDC generated, i.e. not entered by SC)		
<b>Member_ID</b> – IDC always as member id 66		
<b>Subject</b> – A concatenation of flowgate name and TLR level		
<b>TlrLevel</b> – Procedure Level		
<b>FlowGate</b> – Name or description (from book of flowgates)		
<b>FlowGateNumber - Example:</b>		
REGION	TRANSMISSION PROVIDER	FLOWGATE NUMBER RANGE
MAAC	PJM	0001 - 0999
<b>Direction</b> nvarchar(20) <FROM -> TO   TO -> FROM>		
<b>Priority</b> <1,...7> highest priority TLR Level will curtail		
<b>Type</b> <PDTF   ODTF>		
<b>TimeStamp</b> (sent by OATI IDC – effective or valid time TLR event is issued for)		
<b>MessageType</b> (permissions) <SC   CA   SCIS   NERC   PUBLIC   TEST>		
<b>Message</b> (SC enters TLR message or IDC auto-generates for SC,CA,SCIS users)		
<b>PublicMessage</b> (SC enters TLR message or IDC auto-generates for public only)		

### 2.2 Book of Flowgates Additional Fields Considered for OASIS Security Event Template Requirements

A cursory review of the Book of Flowgates, convinces one that the TLR Message cannot utilize the following additional fields found there for OASIS security event template requirements without additional standardization and/or translation efforts.

#### Rationale for Flowgate...cannot be used for FACILITY\_LIMIT\_TYPE

##### Attribute Domain:

Data Checking  
 Voltage Stability  
 Thermal Reliability  
 TVA ties to VACAR  
 Thermal limit  
 Thermal/voltage limit  
 System tie  
 Voltage Stability  
 Thermal,voltage limit  
 Thermal,loadability  
 Pl.View-Dickerson Limit  
 Therm limit,PJM imports

Crit. Conting., sched limit  
 Thermal, Volt, Stability  
 PROVIDE RELIEF FOR TRIMBLE - MIDDLETOWN 345KV OUTAGE  
 phase angle, volt stability  
 thermalreliab; substitute for Lore-Turkey Rvr limits  
 Thermal Limit/Inform.  
 Stability  
 Stability/Thermal  
 Thermal/transient stability limits

Type of Flowgate... cannot be used either
Attribute Domain:
Com
Com, Le
Cont
Info
Inform
Inform, Le
Rel
Rel (OTDF)
Rel (OTDF), Le
Rel (OTDF), Le, MRD
Rel (OTDF), MRD
Rel (OTDF), MRD, Le
Rel, Com
Rel, Cont.
Rel, Le
Rel, MRD
Rel, MRD, Le
Rel, MRD, Le

### 2.3 Recommended Mapping - TLR Message to SecurityPost Template

At this point we recommend constructing an OASIS security event from the existing TLR status message. To construct an event we must first recognize its initial entry in the stream of status messages from the IDC.

#### 2.3.0 The TLR Event-Recognition Procedure

The recognize-event procedure follows:

1. From the current status message obtain its flowgate number and assign it to a variable, say FlowGateNo.
2. Find the latest event level *in the database* that matches this status message's flowgate number. The pseudo-query is:  

```
SELECT TlrLevel
FROM Status_Messages
WHERE FlowGateNumber = FlowGateNo
AND TimeStamp = (SELECT max(TimeStamp) FROM Status_Messages WHERE FlowGateNumber = FlowGateNo)
```
3. If TlrLevel is not found, the current status message is a new event's initial level message. Note: in this case, this is the flowgate's first registered (i.e., recorded-in-the-database) event.
4. If TlrLevel is 0, then the previous event on this flowgate has ended. Recognize the current status message as a new event's initial level message.

This approach checks for latest status messages in the existing TLR status message table. However, we really want to check the conditions against the to-be-defined OASIS security event tables (Section 4.3). The algorithm will be redefined later as a database trigger on the TLR status message table (in Section 5.2); there the recognition of a new event will be determined by the value of the Event Stop Time.

Once an event can be recognized, we can assign it a unique event id.

### 2.3.1 Event ID

Concatenate the event's FlowGateNumber with the TimeStamp attribute from the event's initial level message, separated by an underscore. An event's initial level timestamp is determined from the recognize-event procedure defined above. This effective time becomes the event start time (see below). The format of a TLR event id is NNNNN\_YYYYMMDDHHMMSS where NNNNN lies in the number range defined in the Book of Flowgates and YYYYMMDDHHMMSS is the event start time in Coordinated Universal Time (UTC)<sup>1</sup> translated to Central Standard Time (-6 hrs).

### 2.3.2 Security\_Type

We assume all TLR events are of security type "limit", designated "L". If we cannot assume this, then we will have to ask the IDCWG to include a SecurityType field in the status message from the IDC. OASIS S&CP 1.4 requires this one-character descriptor.

### 2.3.2 Initiating\_Party

Under NERC's TLR procedure the CA on the side of the flowgate that's causing the constraint may initiate an event by calling the SC for relief. Otherwise, an SC may initiate the event. This is the CA field in the status message from the IDC (see Section 2.1 above). This 4-character optional code must match a CA or SC code found in the Master Registry at NERC's TSIN registration site.

### 2.3.4 Responsible\_Party

Under NERC's TLR procedure the SC is always the responsible party. This is the SC field in the status message from the IDC (see Section 2.1 above). This required code must match an SC code found in the Master Registry at NERC's TSIN registration site. According to the S&CP it can be up to 25 characters but the 4-character code should be matched.

### 2.3.5 Procedure\_Name

We assume all TLR events will be associated with the "NERC TLR" procedure name. Therefore no attribute in the IDC status message is mapped to this attribute. This matches the registered procedure by the same name in the Master Registry at NERC's TSIN registration site.

### 2.3.6 Procedure\_Level

The PROCEDURE\_LEVEL in the securitypost input template is equated to the TlrLevel data element in the IDC status message. Procedure levels are not part of the Master Registry. However, the description included with the procedure name in the Master Registry contains a list of procedure levels. There is no requirement to match descriptive entries.

### 2.3.7 Facility\_Class

We assume all TLR events will be associated with the "FLOWGATE" facility class. Therefore no attribute in the IDC status message is mapped to this data item.

### 2.3.8 Facility\_Limit\_Type

We assume all TLR events will be associated with the "THERMAL" facility limit type. (Note: we cannot derive this from the Book of Flowgates as discussed in Section 2.2.) If not, then we will have to ask the IDCWG to include a FacilityLimitType field in the status message from the IDC to determine this for us. However the S&CP says it is optional; hence, it can be left blank if "THERMAL" is misleading to the industry. No attribute in the IDC status message is mapped to this data item at this time.

### 2.3.9 Facility\_Location

We assume all TLR events will be associated with the "EXTERNAL" facility\_location. If not, and the industry majority rules that it depends on whether the flowgate is internal or external to a particular transmission provider's service territory, then it should be left blank in the Central Repository. Under this scenario, it will be left up to the transmission provider, when posting the security event, to

---

<sup>1</sup> Coordinated Universal Time (UTC) is broadcast on satellites, on the Internet and on stations such as WWV. It was adopted internationally in February 1971 to become effective January 1, 1972. The clock rate is controlled by atomic clocks to be as uniform as possible for one year, but is changed by the infrequent addition or deletion of a second – called a "leap second" so that UTC never differs more than 0.7 sec from the navigator's time scale, UT1. UT1 is Universal Time (UT0) corrected for the wobble of the earth on its axis (?t ~ 0.05 sec). UT0 is based on the count of days as they actually occurred historically; in other words on the actual spin of the earth on its axis; historically, on mean solar time (solar position as corrected by the "equation of time"; i.e., the faster travel of the earth when near the sun than when far from the sun) as determined at Greenwich Observatory. – abstracted in Charles W. Misner, Kip S. Thorne and John Archibald Wheeler's *GRAVITATION*, from Barnes, J.A., 1971, "A non-mathematical discussion of some basic concepts of precise time measurement," in *Tracor on Frequency* 2, No. 2 (Tracor Industrial Instruments, Austin, Texas).

supply the designation. One can argue that all TLR events are external however, since a flowgate has two sides, where at least one side is external to a given provider. The S&CP says it is optional; hence, it can be left blank if “EXTERNAL” is misleading to the industry. No attribute in the IDC status message is mapped to this data item at this time.

### 2.3.10 Facility\_Name

The FACILITY\_NAME in the securitypost input template is equated to the FlowGate data element in the IDC status message. This field contains the name of the flowgate from the Book of Flowgates. Since the Book of Flowgates is not in NERC’s Master Registry there is no matching requirement. The S&CP states that FACILITY\_NAME is optional and has a length of 25 characters. It has been recommended that 100 characters be used before truncation, because the names are often longer than 25 and sometimes greater than 50 characters, but never longer than 100. The IDC status message field itself allows up to 255 characters. We recommend the mapping use up to the first 100 characters.

### 2.3.11 Start\_Time

The START\_TIME (YYYYMMDDHHMMSSTZ) in the securitypost input template is equated to the TimeStamp data element in the IDC status message. This field contains the effective or valid time of the event level in Central Standard Time (TimeZone appended to date and time is CS). Upon upload to OASIS it will be translated from Central Standard Time to Greenwich Mean Time (+6 hrs), as all times on OASIS are stored in GMT. If it is the initial event level, i.e. recognized as a new event, then it is considered *the start time of the event* as well. If the status message TlrLevel is 0, then it is considered *the stop time of the event* as well. The implications that follow from this mapping are realized in the database schema design in Section 4.

This completes the mapping between the IDC status message and the recommended OASIS securitypost input template.

## 2.4 Additional Information to be Posted in the NERC TLR Logs

The Security Coordinator will enter the following additional information on the TLR Log report form. This event level information is to be made available to Customers at the NERC TLR Log Web Site:

2. The present flow on the constrained flowgate
3. The post-contingent flow on the constrained flowgate
4. The MW limit on the constrained flowgate
5. The present flow on the contingent flowgate
6. Comments about actions taken
7. Description of initial conditions exacerbating the problem

Once the Security Coordinator has terminated the TLR event by issuing a TLR level 0, the IDC will remind the Security Coordinator to terminate the TLR Log report and request that it be sent to the NERC ftp and web sites.

## SECTION 3. Mapping WSCC USF Excerpts to OASIS Security Event Template Items

This section develops the mapping of WSCC's Unscheduled Flow Reduction Procedure information to OASIS information. Currently WSCC uses email to communicate between transfer path operators the USF reduction action steps of the Western Interconnection reduction procedure on qualified paths. A form is completed and sent via email to WSCC security coordinators and WSCC Staff. This form shall be forwarded to NERC by WSCC Staff on behalf of the WSCC Unscheduled Flow Administrative Subcommittee (USAF) as the security event information for the OASIS security template in complying with FERC Order 605. The WSCC email system is the only system that can supply the NERC Central Repository with data generated by WSCC's USF Reduction Procedure for the Western Interconnection (Policy 9, Appendix 9C2). The method will make use of a push-based delivery mode to the NERC Central Repository, using the email system.

### 3.1 WSCC USF Email Message Data Elements

The following USF Reduction Procedure form contents shall be sent from WSCC to NERC for each action step:

<b>WSCC USF Email Status Message to NERC</b>			
<b>From</b> – Transfer Path Operator <TSIN – registered four character code>			
<b>Subject</b> – <"Unscheduled Flow Reduction Procedure">			
<b>ActionRequired</b> – Action required/ no action required (alert only) – Check box <0,1>			
<b>Path</b> – <Qualified Path Id from WSCC USAF's list of qualified paths>			
<b>Status</b> – ??			
<b>InstantaneousFlow</b> – MWs of path's instantaneous flow			
<b>TransferCapability</b> – MWs of path's transfer capability at time of message			
<b>ScheduleAcrossPath</b> – MWs of schedule across the path at time of message			
<b>TypeOfRequest</b> – A concatenation of : (Check the following that apply) < n <sub>1</sub> n <sub>2</sub> n <sub>3</sub> n <sub>4</sub> n <sub>5</sub> n <sub>6</sub> n <sub>7</sub> n <sub>8</sub> > where n <sub>1</sub> is check box 1, etc <del>1.</del> 1.) PATH OPERATOR HAS MET ALL ACCOMODATION REQUIREMENTS AND OPERATED AVAILABLE INDEPENDENT CONTROLLABLE DEVICE.  ACTION REQUIRED <del>2.</del> 2.) START COORDINATED CONTROLLABLE DEVICE OPERATION <del>3.</del> 3.) CONTINUE COORDINATED CONTROLLABLE DEVICE OPERATION <del>4.</del> 4.) TERMINATE COORDINATED CONTROLLABLE DEVICE OPERATION  <del>5.</del> 5.) START INDICATED LEVEL OF SCHEDULE CURTAILMENTS <del>6.</del> 6.) CONTINUE PRESENT LEVEL OF SCHEDULE REDUCTIONS <del>7.</del> 7.) CHANGE LEVEL OF SCHEDULE REDUCTIONS <del>8.</del> 8.) TERMINATE SCHEDULE CURTAILMENTS			
<b>BeginTime</b> –time schedule curtailments are to begin (hour-ending) _____ (Zone) Note: Only If 5 or 7 is checked above.			
<b>ActionStep</b> <4-9> :			
<del>1.</del>	FIRST LEVEL (STEP 4)	50% OR GREATER 30 - 49%	20% 10%
<del>2.</del>	SECOND LEVEL (STEP 5)	50% OR GREATER 30 - 49% 20 - 29%	25% 15% 10%
<del>3.</del>	THIRD LEVEL (STEP 7)	50% OR GREATER 30 - 49% 20 - 29% 15 - 19%	30% 20% 15% 10%
<del>4.</del>	FOURTH LEVEL (STEP 9)	50% OR GREATER 30 - 49% 20 - 29% 15 - 19% 10 - 14%	35% 25% 20% 15% 10%
<b>Comments</b> <255 characters>			

## 3.2 Recommended Mapping - USF Message to SecurityPost Template

At this point we recommend constructing an OASIS security event from the USF email message. To construct an event we must first recognize its initial entry in the stream of status messages from the WSCC.

### 3.2.0 The USF Reduction Event-Recognition Procedure

The recognize-event procedure follows:

1. From the current status message, obtain its TypeOfRequest and PathId. Assign PathId to a variable, say PathNo.
8. If TypeOfRequest( $n_5$ ) is equal to 1 (i.e. the box -- START INDICATED LEVEL OF SCHEDULE CURTAILMENTS -- is checked), the current status message is a new reduction event's initial action step message.
9. Verify that the previous Action Step record in the database, where PathId = PathNo, contains TypeOfRequest( $n_8$ ) is equal to 1 (i.e. the box -- TERMINATE SCHEDULE CURTAILMENTS -- is checked). This verifies that the previous USF Reduction event *on this qualified path* has been terminated.

Once an event can be recognized, we can assign it a unique event id.

#### 3.2.1 Event ID

Concatenate the event's PathId with the BeginTime attribute from the event's initial action step message, separated by an underscore. An event's initial action step begin time is determined from the recognize-event procedure defined above. This effective time becomes the event start time (see below). The format of a USF reduction event id is NN\_YYYYMMDDHHMMSS where NN lies in the number range defined in the List of Qualified Paths and YYYYMMDDHHMMSS is the event start time in Coordinated Universal Time (UTC)<sup>2</sup> translated to Central Standard Time (-6 hrs).

#### 3.2.2 Security\_Type

We assume all USF reduction events are of security type "limit", designated "L". If we cannot assume this, then we will have to ask the WSCC USAF to include a SecurityType field in the status message from the WSCC. OASIS S&CP 1.4 requires this one-character descriptor.

#### 3.2.2 Initiating\_Party

Under WSCC's USF reduction procedure the transfer path operator whose qualified path is experiencing the constraint initiates a reduction event by calling for relief. The initiating TP/CA is determined by the status message's From data element, which will be a 4-character code. These 4-character codes must match a TP or CA code found in the Master Registry at NERC's TSIN registration site.

#### 3.2.4 Responsible\_Party

Under WSCC's USF reduction procedure the initiating party is the responsible party as well. See Section 3.2.2.

#### 3.2.5 Procedure\_Name

We assume all USF events will be associated with the "WSCC\_USF" procedure name. Therefore no attribute in the USF Reduction status message is mapped to this attribute. This matches the registered procedure by the same name in the Master Registry at NERC's TSIN registration site.

#### 3.2.6 Procedure\_Level

The PROCEDURE\_LEVEL in the securitypost input template is equated to the ActionStep data element in the USF status message. Procedure levels are not part of the Master Registry. However, the description included with the procedure name in the Master Registry contains a list of procedure levels. There is no requirement to match descriptive entries.

#### 3.2.7 Facility\_Class

We assume all USF reduction events will be associated with the "QUALIFIED\_PATH" facility class. Therefore no attribute in the USF status message is mapped to this data item.

#### 3.2.8 Facility\_Limit\_Type

We assume all USF events will be associated with the "THERMAL" facility limit type. If not, then we will have to ask the WSCC USAF to include a FacilityLimitType field in the status message from the USF to determine this for us. However the S&CP says it is

---

<sup>2</sup> See Section 2.3.1.

optional; hence, it can be left blank if “THERMAL” is misleading to the industry. No attribute in the USF reduction status message is mapped to this data item at this time.

### 3.2.9 Facility\_Location

We assume all USF events will be associated with the “EXTERNAL” facility\_location. If not, and the industry majority rules that it depends on whether the qualified path is internal or external to a particular transfer path operator’s service territory, then it should be left blank in the Central Repository. Under this scenario, it will be left up to the transmission provider, when posting the security event, to supply the designation. One can argue that all USF reduction events are external however, since a qualified path has two endpoints, where at least one is external to a given provider. The S&CP says it is optional; hence, it can be left blank if “EXTERNAL” is misleading to the industry. No attribute in the USF status message is mapped to this data item at this time.

### 3.2.10 Facility\_Name

The FACILITY\_NAME in the securitypost input template is derived from the PathId data element in the USF status message. As with the Initiating Party (Section 3.2.2), this field is derived from the PathId using the WSCC\_Qualified\_Path\_Facility Table in the NERC database. It will contain the long name of each qualified path from the WSCC USAF’s list of qualified paths. Since the list of qualified paths is not in NERC’s Master Registry there is no matching requirement. The S&CP states that FACILITY\_NAME is optional and has a length of 25 characters. It has been recommended that 50 characters be used.

### 3.2.11 Start\_Time

The START\_TIME in the securitypost input template is equated to the BeginTime data element in the USF reduction status message. This field contains the effective or valid time of the event level in Central Standard Time, and must be translated (+6 hrs) from Central Standard Time to Greenwich Mean Time, as all times on OASIS are stored in GMT. If it is the initial event action step, i.e. recognized as a new event (Section 3.2.0), then it is considered *the start time of the event* as well. If the status message TypeOfRequest(n<sub>8</sub>) is 1, then it is considered *the stop time of the event* as well. The implications that follow from this mapping are realized in the database schema design in Section 4.

This completes the mapping between the USF email message and the recommended OASIS securitypost input template.

## SECTION 4. A Database Schema for Security Events Built from IDC TLR Status and USF Action Step Messages.

### 4.1 Existing NERC IDC TLR Status Message Table in the Central Repository Database

The following table in the Central Repository database at NERC represents the IDC TLR status message.

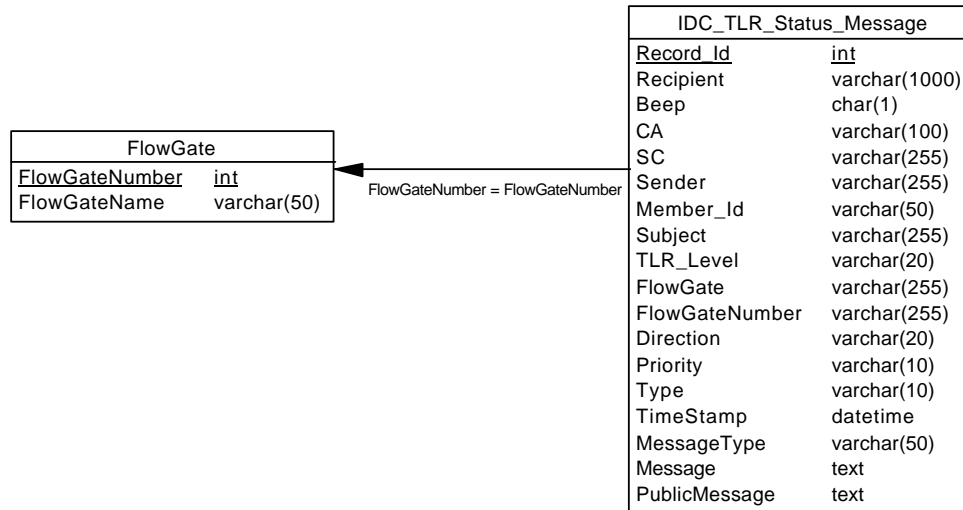


Figure 1. IDC TLR Message Table in the CRC

### 4.2 Proposed WSCC USF Reduction Message Tables in the Central Repository Database

The following tables in the Central Repository database at NERC represent the USF reduction status message.

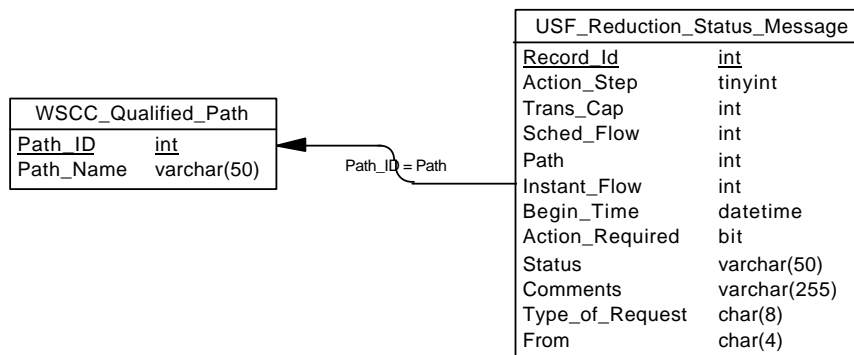
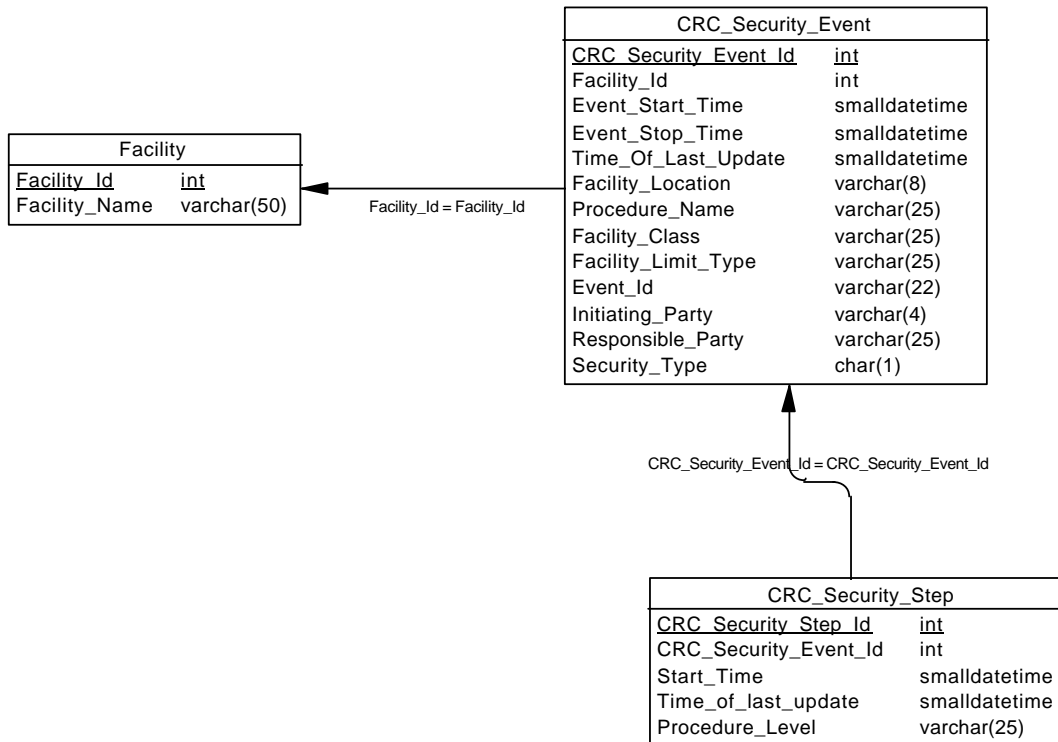


Figure 2. WSCC USF Reduction Procedure Message Tables in the CRC

### 4.3 Proposed Security Event Tables in the Central Repository Database

The following database schema organizes IDC TLR status messages and USF reduction procedure action step email messages into an historical record of major transmission security events. The Central Repository tables needed for the new requirements are as follows:



**Figure 3. Security Event Tables in the CRC**

The CRC\_Security\_Event and CRC\_Security\_Step tables shall be filled from the IDC\_TLR\_Status and USF\_Reduction\_Status Message tables as follows:

- ?? Define insert and update triggers on both the IDC\_TLR\_Status and USF\_Reduction\_Status\_Message tables such that when a new message record is inserted or updated, a corresponding security step and, if a new event, a corresponding security event is inserted in the CRC OASIS Security Event tables.
- ?? Translations between message tables and security event tables are defined in Sections 2.1 and 3.1
- ?? Trigger for TLR level insert:

```

CREATE TRIGGER Insert_TLR_Level ON dbo.IDC_TLR_Status_Message
FOR INSERT
AS
DECLARE
    @Record_id int,
    @Event_id varchar(22),
    @CA varchar(4),
    @SC varchar(25),
    @FlowgateNumber int,
    @TimeStamp smalldatetime,
    @TLR_Level varchar(20)

DECLARE cursor_on_Inserted CURSOR
FOR
    SELECT Record_Id,
           FlowGateNumber + '_' + convert(char(8),TimeStamp,112) + convert(char(2),TimeStamp,8) +
           right(convert(char(5),TimeStamp,8),2) + right(convert(char(8),TimeStamp,8),2),
           CA,SC,FlowGateNumber,TimeStamp,TLR_Level
    FROM inserted
OPEN cursor_on_Inserted
FETCH NEXT FROM cursor_on_Inserted
    INTO @Record_id, @Event_id, @CA, @SC, @FlowgateNumber, @TimeStamp, @TLR_Level
    
```

```

DEALLOCATE cursor_on_inserted
---If there exists no previous TLR event for this flowgate
---then insert a new event record in table CRC_Security_Event.
SELECT CRC_Security_Event_Id
FROM CRC_Security_Event C
WHERE C.Facility_Id = @FlowGateNumber
IF @@ROWCOUNT = 0
    INSERT INTO CRC_Security_Event
    (CRC_Security_Event_Id, Event_Id, Initiating_Party, Responsible_Party, Facility_id,
    Event_Start_Time, Time_Of_Last_Update)
    VALUES ( @Record_id, @Event_id, @CA, @SC, @FlowgateNumber, @TimeStamp, getdate() )
ELSE
---assume the database default for Event_Stop_Time -- 6/6/2079 - is used to initialize Event Stop Time
---If there does not exist a previous TLR event on this flowgate whose Event_Stop_Time is 6/6/2079
---i.e., all events have real endings
---then insert a new event record in table CRC_Security_Event.
BEGIN
    SELECT Event_Stop_Time
    FROM CRC_Security_Event C
    WHERE C.Facility_Id = @FlowGateNumber
    AND C.Event_Stop_Time = '6/6/2079' --- i.e., the default for no event stop time
    IF @@ROWCOUNT = 0
        INSERT INTO CRC_Security_Event
        (CRC_Security_Event_Id, Event_Id, Initiating_Party, Responsible_Party, Facility_id,
        Event_Start_Time, Time_Of_Last_Update)
        VALUES ( @Record_id, @Event_id, @CA, @SC, @FlowgateNumber, @TimeStamp, getdate() )
END

---insert a new level record in table CRC_Security_Step
INSERT INTO CRC_Security_Step
(CRC_Security_Step_Id, CRC_Security_Event_Id, Procedure_Level, Start_Time, Time_Of_Last_Update)
VALUES ( @Record_id, @Record_id, @TLR_Level, @TimeStamp, getdate() )

---if TLR_Level = 0 then update CRC_Security_Event's Event_Stop_Time
IF @TLR_Level = '0'
    UPDATE CRC_Security_Event
    SET Event_Stop_Time = @TimeStamp, Time_Of_Last_Update = getdate()
    WHERE CRC_Security_Event_Id = @Record_id

```

#### 4.4 Attributes of Security Event and Security Step Tables in the Central Repository Database

The attributes of the Security Event and Security Step Tables are listed below:

<p><b>CRC_SECURITY_EVENT_ID</b>  <u>Required</u> – NERC TLR or USF ID No. + EVENT_START_TIME  17{UPALPHANUM}20 (Time is in Central Standard Time)  NN_YYYYMMDDHHMMSS (for WSCC)  NNNNN_YYYYMMDDHHMMSS (for NERC)</p>
<p><b>SECURITY_TYPE</b>  <u>Required</u> 1{Alphanumeric}  &lt;"L" for LIMIT   "O" for OUTAGE&gt;</p>
<p><b>INITIATING_PARTY</b>  <u>Optional</u> – CA or TP Code 0{Alphanumeric}4</p>
<p><b>RESPONSIBLE_PARTY</b>  <u>Required</u> – SC or CA or TP Code 1{Alphanumeric}25</p>
<p><b>PROCEDURE_NAME</b>  <u>Required</u> – TLR or registered procedure 1{Alphanumeric}25  Registered Procedure Name</p>
<p><b>PROCEDURE_LEVEL</b>  <u>Required</u> – 1{Alphanumeric}25  Registered Level Dependent on PROCEDURE_NAME, e.g, TLR  Level or USF Action Steps 4 through 9</p>
<p><b>FACILITY_CLASS</b>  <u>Optional</u> 0{Alphanumeric}25  "FLOWGATE", "LINE", etc.</p>
<p><b>FACILITY_LIMIT_TYPE</b>  <u>Optional</u> 0{Alphanumeric}25  "THERMAL", "STABILITY", etc.</p>
<p><b>FACILITY_LOCATION</b>  <u>Optional</u> 0{Alphanumeric}8  "INTERNAL" or "EXTERNAL"</p>
<p><b>FACILITY_NAME</b>  <u>Required</u> 1{Alphanumeric}25 – Note: Recommended Change - 50  Path or Flowgate name</p>
<p><b>FACILITY_ID</b>  <u>Required</u> 2{Numeric}5  Registered Flowgate number or USF Path ID number</p>
<p><b>EVENT_START_TIME</b>  <u>Required</u> – Start time of the event. Used to construct  CRC_SECURITY_EVENT_ID.  YYYYMMDDHHMMSSTZ</p>
<p><b>START_TIME</b>  <u>Required</u> – Start time of the level changes.  YYYYMMDDHHMMSSTZ</p>
<p><b>STOP_TIME</b> – Stop time of the level changes.  <u>Optional</u> 16{UPALPHANUM}16  YYYYMMDDHHMMSSTZ</p>
<p><b>EVENT_STOP_TIME</b>  <u>Required</u> at close of event – 16{UPALPHANUM}16  YYYYMMDDHHMMSSTZ</p>
<p><b>TIME_OF_LAST_UPDATE</b>  <u>Optional</u> – On query only 16{UPALPHANUM}16  YYYYMMDDHHMMSSTZ</p>

## SECTION 5. Security Events Distribution – NERC Web-based Application

Having extended the Central Repository database to include a running history of TLR events, the following specifies a NERC web-based application for distribution of security events to OASIS Nodes. The application should provide for security events distribution in a number of ways, as the means and wherewithal of each TP varies. There should be a mechanism for TPs who have set up communication protocols compliant with the S&CP to access and download the needed information at NERC. There should be an additional method utilizing the transaction messaging protocol (TMP) of the E-Tagging System with TP forwarding URL, for those TPs who desire an automated messaging approach. There should be a call-level interface for those TPs who desire a direct programming interface.

### 5.1 Site for Polling and Pull-based Applications

[This has lower priority for March 1<sup>st</sup> than 5.2, as agreed at the Jan 9<sup>th</sup> OSC Meeting.] This deliverable provides a site containing security event information for downloading in the form of CSV files that contain the securitypost input template for upload to OASIS.

Proposed filename convention at NERC Security Template Download Site for NERC TLR security events is **NERC\_TLR\_EventId.csv**. Proposed filename convention at NERC Security Template Download Site for WSCC USF security events is: **WSCC\_USF\_EventId.csv**.

Note that old extracts get overwritten, as new extracts for the same security event are published at the NERC site. Each published extract should be for a singular TLR and should be cumulative over time in regards to TLR Level or USF Action Step Changes.

#### 5.1.1 NERC TLR Example

Extract published on the Download Site, excerpt sent from IDC to the NERC TLR Web Site Database at 8:32 on 11/12/2000

```
VERSION=1.4
TEMPLATE=securitypost
OUTPUT_FORMAT=DATA
PRIMARY_PROVIDER_CODE=
PRIMARY_PROVIDER_DUNS=
RETURN_TZ=CS
DATA_ROWS=1
COLUMN_HEADERS=EVENT_ID,SECURITY_TYPE,INITIATING_PARTY,RESPONSIBLE_PARTY,
PROCEDURE_NAME,PROCEDURE_LEVEL,FACILITY_CLASS,FACILITY_LIMIT_TYPE,FACILITY_LOCATION,
FACILITY_NAME,START_TIME
9084,L,IMO,IMO,TLR,1,FLOWGATE,THERMAL,EXTERNAL,MECS-IMO,20001112083100CS
```

Extract published on the Download Site, excerpt sent from IDC to the NERC TLR Web Site Database at 9:27 on 11/12/2000

```
VERSION=1.4
TEMPLATE=securitypost
OUTPUT_FORMAT=DATA
PRIMARY_PROVIDER_CODE=
PRIMARY_PROVIDER_DUNS=
RETURN_TZ=CS
DATA_ROWS=2
COLUMN_HEADERS=EVENT_ID,SECURITY_TYPE,INITIATING_PARTY,RESPONSIBLE_PARTY,
PROCEDURE_NAME,PROCEDURE_LEVEL,FACILITY_CLASS,FACILITY_LIMIT_TYPE,FACILITY_LOCATION,
FACILITY_NAME,START_TIME
9084,L,IMO,IMO,TLR,1,FLOWGATE,THERMAL,EXTERNAL,MECS-IMO,20001112083100CS
9084,L,IMO,IMO,TLR,3A,FLOWGATE,THERMAL,EXTERNAL,MECS-IMO,20001112100000CS
```

Extract published on the Download Site, excerpt sent from IDC to the NERC TLR Web Site Database at 10:29 on 11/12/2000

```
VERSION=1.4
TEMPLATE=securitypost
OUTPUT_FORMAT=DATA
PRIMARY_PROVIDER_CODE=
PRIMARY_PROVIDER_DUNS=
RETURN_TZ=CS
```

DATA\_ROWS=3  
COLUMN\_HEADERS=EVENT\_ID,SECURITY\_TYPE,INITIATING\_PARTY,RESPONSIBLE\_PARTY,  
PROCEDURE\_NAME,PROCEDURE\_LEVEL,FACILITY\_CLASS,FACILITY\_LIMIT\_TYPE,FACILITY\_LOCATION,  
FACILITY\_NAME,START\_TIME  
9084 ,L , IMO , IMO , TLR , 1 , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112083100CS  
9084 ,L , IMO , IMO , TLR , 3A , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112100000CS  
9084 ,L , IMO , IMO , TLR , 3A , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112110000CS

---  
---  
---  
Extract published on the Download Site, excerpt sent from IDC to the NERC TLR Web Site Database at 15:24 on 11/12/2000  
VERSION=1.4

TEMPLATE=securitypost  
OUTPUT\_FORMAT=DATA  
PRIMARY\_PROVIDER\_CODE=  
PRIMARY\_PROVIDER\_DUNS=  
RETURN\_TZ=CS  
DATA\_ROWS=8  
COLUMN\_HEADERS=EVENT\_ID,SECURITY\_TYPE,INITIATING\_PARTY,RESPONSIBLE\_PARTY,  
PROCEDURE\_NAME,PROCEDURE\_LEVEL,FACILITY\_CLASS,FACILITY\_LIMIT\_TYPE,FACILITY\_LOCATION,  
FACILITY\_NAME,START\_TIME  
9084 ,L , IMO , IMO , TLR , 1 , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112083100CS  
9084 ,L , IMO , IMO , TLR , 3A , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112100000CS  
9084 ,L , IMO , IMO , TLR , 3A , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112110000CS  
9084 ,L , IMO , IMO , TLR , 3A , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112120000CS  
9084 ,L , IMO , IMO , TLR , 3A , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112130000CS  
9084 ,L , IMO , IMO , TLR , 3A , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112140000CS  
9084 ,L , IMO , IMO , TLR , 3A , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112150000CS  
9084 ,L , IMO , IMO , TLR , 0 , FLOWGATE , THERMAL , EXTERNAL , MECS-IMO , 20001112152400CS

## 5.1.2 WSCC USF Example

Excerpt sent from WSCC to the NERC Security Template Download Site at 8:32 on 11/12/2000  
VERSION=1.4

TEMPLATE=securitypost  
OUTPUT\_FORMAT=DATA  
PRIMARY\_PROVIDER\_CODE=  
PRIMARY\_PROVIDER\_DUNS=  
RETURN\_TZ=CS  
DATA\_ROWS=1  
COLUMN\_HEADERS=EVENT\_ID,SECURITY\_TYPE,INITIATING\_PARTY,RESPONSIBLE\_PARTY,  
PROCEDURE\_NAME,PROCEDURE\_LEVEL,FACILITY\_CLASS,FACILITY\_LIMIT\_TYPE,FACILITY\_LOCATION,  
FACILITY\_NAME,START\_TIME  
133212 ,L , WAPA , WAPA , WSCC\_USF , 4 , QUALIFIED\_PATH , THERMAL , EXTERNAL , WAPA-MPCO ,  
20001112083100CS

Excerpt sent from WSCC to the NERC Security Template Download Site at 9:27 on 11/12/2000  
VERSION=1.4

TEMPLATE=securitypost  
OUTPUT\_FORMAT=DATA  
PRIMARY\_PROVIDER\_CODE=  
PRIMARY\_PROVIDER\_DUNS=  
RETURN\_TZ=CS  
DATA\_ROWS=2  
COLUMN\_HEADERS=EVENT\_ID,SECURITY\_TYPE,INITIATING\_PARTY,RESPONSIBLE\_PARTY,  
PROCEDURE\_NAME,PROCEDURE\_LEVEL,FACILITY\_CLASS,FACILITY\_LIMIT\_TYPE,FACILITY\_LOCATION,  
FACILITY\_NAME,START\_TIME  
133212 ,L , WAPA , WAPA , WSCC\_USF , 4 , QUALIFIED\_PATH , THERMAL , EXTERNAL , WAPA-MPCO , 20001112083100CS  
133212 ,L , WAPA , WAPA , WSCC\_USF , 5 , QUALIFIED\_PATH , THERMAL , EXTERNAL , WAPA-MPCO , 20001112100000CS

Excerpt sent from WSCC to the NERC Security Template Download Site at 10:29 on 11/12/2000  
VERSION=1.4

```

TEMPLATE=securitypost
OUTPUT_FORMAT=DATA
PRIMARY_PROVIDER_CODE=
PRIMARY_PROVIDER_DUNS=
RETURN_TZ=CS
DATA_ROWS=3
COLUMN_HEADERS=EVENT_ID,SECURITY_TYPE,INITIATING_PARTY,RESPONSIBLE_PARTY,
PROCEDURE_NAME,PROCEDURE_LEVEL,FACILITY_CLASS,FACILITY_LIMIT_TYPE,FACILITY_LOCATION,
FACILITY_NAME,START_TIME
133212,L,WAPA,WAPA,WSCC_USF,4,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112083100CS
133212,L,WAPA,WAPA,WSCC_USF,5,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112100000CS
133212,L,WAPA,WAPA,WSCC_USF,6,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112110000CS
---
```

Final excerpt sent from WSCC to the NERC Security Template Download Site at 15:24 on 11/12/2000

```

VERSION=1.4
TEMPLATE=securitypost
OUTPUT_FORMAT=DATA
PRIMARY_PROVIDER_CODE=
PRIMARY_PROVIDER_DUNS=
RETURN_TZ=CS
DATA_ROWS=8
COLUMN_HEADERS=EVENT_ID,SECURITY_TYPE,INITIATING_PARTY,RESPONSIBLE_PARTY,
PROCEDURE_NAME,PROCEDURE_LEVEL,FACILITY_CLASS,FACILITY_LIMIT_TYPE,FACILITY_LOCATION,
FACILITY_NAME,START_TIME
133212,L,WAPA,WAPA,WSCC_USF,4,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112083100CS
133212,L,WAPA,WAPA,WSCC_USF,5,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112100000CS
133212,L,WAPA,WAPA,WSCC_USF,6,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112110000CS
133212,L,WAPA,WAPA,WSCC_USF,7,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112120000CS
133212,L,WAPA,WAPA,WSCC_USF,8,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112130000CS
133212,L,WAPA,WAPA,WSCC_USF,9,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112140000CS
133212,L,WAPA,WAPA,WSCC_USF,8,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112150000CS
133212,L,WAPA,WAPA,WSCC_USF,4,QUALIFIED_PATH,THERMAL,EXTERNAL,WAPA-MPCO,20001112152400CS
```

## 5.2 OASIS S&CP security Template at NERC CRC – for Polling and Pull-based Applications

[This has highest priority for March 1<sup>st</sup>] The OASIS S&CP-based application essentially will mimic the Query/Response functionality of the security template defined in S&CP 1.4 as required for an OASIS Node. The only difference at the NERC CRC Site is that the Output Format most likely will be set equal to DATA by the transmission provider-as-customer, so that it can be turned around and uploaded to the provider’s own OASIS Site. It is also expected that CSV downloads of *multiple* security events, based on a subset of Query Filter Value Pairs will be commonplace. NERC Security Template Web Pages will provide both Display and Data Output at:

<http://crc.nerc.com>

## 5.3 Call-Level Interface Programmatic API for Polling and Pull-based Applications

[This is not for March 1<sup>st</sup>.]

## 5.4 SECURITYPOST TMP Message with TP Forwarding URL -- Push-based Application

[This is not for March 1<sup>st</sup>.] For those TPs supplying TP forwarding URLs in the Master Registry to implement Security Event Notification via the SECURITYPOST TMP Message, the following requirements shall apply:

- ?? A TMP listener or data service that meets the E-Tag 1.66.02 specs for Tag Agent Notification -- but without “Authentication Key” requirements -- must reside at the TP forwarding URL.
- ?? The NERC CRC Notification Service will initiate and perform the required number of attempts, within the required range of time, specified in the E-Tag spec for Tag Authorities, to communicate with the listener or data service.
- ?? It is impossible at this time to distinguish security events relative to a particular transmission provider, except perhaps by Interconnection. Hence, the TP supplying a TP forwarding URL should be prepared to receive notification of *all* security events in a given Interconnection.

## **5.5 SECURITYPOST Direct CSV Upload at TP Forwarding URL -- Push-based Application**

[This is not for March 1<sup>st</sup>.]

## SECTION 6. TP Tag Forwarding for Adjustments to be Sent to OASIS Nodes to Supply security and scheduledetail Templates

[This is not for March 1<sup>st</sup>.] This is a proposal for sending appropriate OASIS Nodes the information required in complying with FERC Order 605. Use of the E-Tagging system is necessary for data delivery, because it is the only system which can distinguish which OASIS nodes are tied to an adjusted interchange transaction. The method makes use of a push-based delivery mode and is in lieu of a fully developed central repository, which is not projected to be completed until Fall of 2001. It also allows non-Eastern Interconnection TLR curtailment events, such as WSCC Unscheduled Flow Reduction (NERC Policy 9, Appendix 9C2), ERCOT actions (Appendix 9C3) and local curtailment events to be disseminated to the appropriate OASIS Nodes.

1. Add to the TP\_Registry a Method Attribute to be used to determine whether CURTAIL\_POST TMP Message is to be used or an OASIS curtailpost CSV Upload is to be used. Method attribute values are 'TMP' and 'OASIS'.
2. Change the Master Registry's TP\_Registry attribute, Forward\_URL, from Invalid to Optional. If the 'OASIS' method is used, the TP forwarding service should be set to the TP's OASIS Home directory:

"http://(oasis node name):Port/OASIS/Primary\_Provider\_Code.

Note the distinction between **CA Tag Forwarding** (Step 4 in diagram below), in which the Load Control Area's forward service in the Master Registry is used, and **TP Tag Adjust Forwarding** (Step 6), in which the TP's forward service is used.

3. On an adjustment, for each TP in the Transaction Path for the tag, the LCA Tag Authority Service examines the Master Registry and verifies that the listed TP has a forwarding URL defined. If not, the Tag Forwarding process continues with the next TP.
4. If the Tag Forwarding URL is present, the Tag Authority Service should modify the Entity State of the appropriate "TP" record in the STATUS table as PENDING.
5. If the service responds with a SUCCESS message, the Tag Authority Service shall set the Entity State to APPROVED.
6. If the service responds with a FAIL message, the Tag Authority Service shall set the Entity State to INVALID and the first 80 characters of the error message after the word FAIL shall be placed in the Reason Field.

Figure 1 below shows five existing steps and a sixth proposed step for adjusting tags.

**Step 1 – the Adjustment Notification Step** -- occurs only when the curtailment originates from the IDC, used by NERC's TLR Procedure (Policy 9, Appendix 9C1). An example follows:

```
ADJUST_LIST ISNE IDC1234567890AB 9084 11/12/2000 14:31 IMO
"PJM_PECOENAYA19DH_ISNE",11/12/2000 15:00,11/30/2000 23:00,39,,"TLR Level 3A on flowgate 9084 at 11/12/2000 14:31:00 (CST)"
ADJUST_LIST_END
```

Where:

```
ADJUST_LIST <Target Entity> <Authentication Key> <Flowgate> <DateTime> <Issuer>
"<Tag ID> ", <Adjust Start DateTime>, <Adjust Stop DateTime>, <MW Cap>, <Operator Id>,"<Reason>"
No changes to the 1.66 spec are needed for this.
```

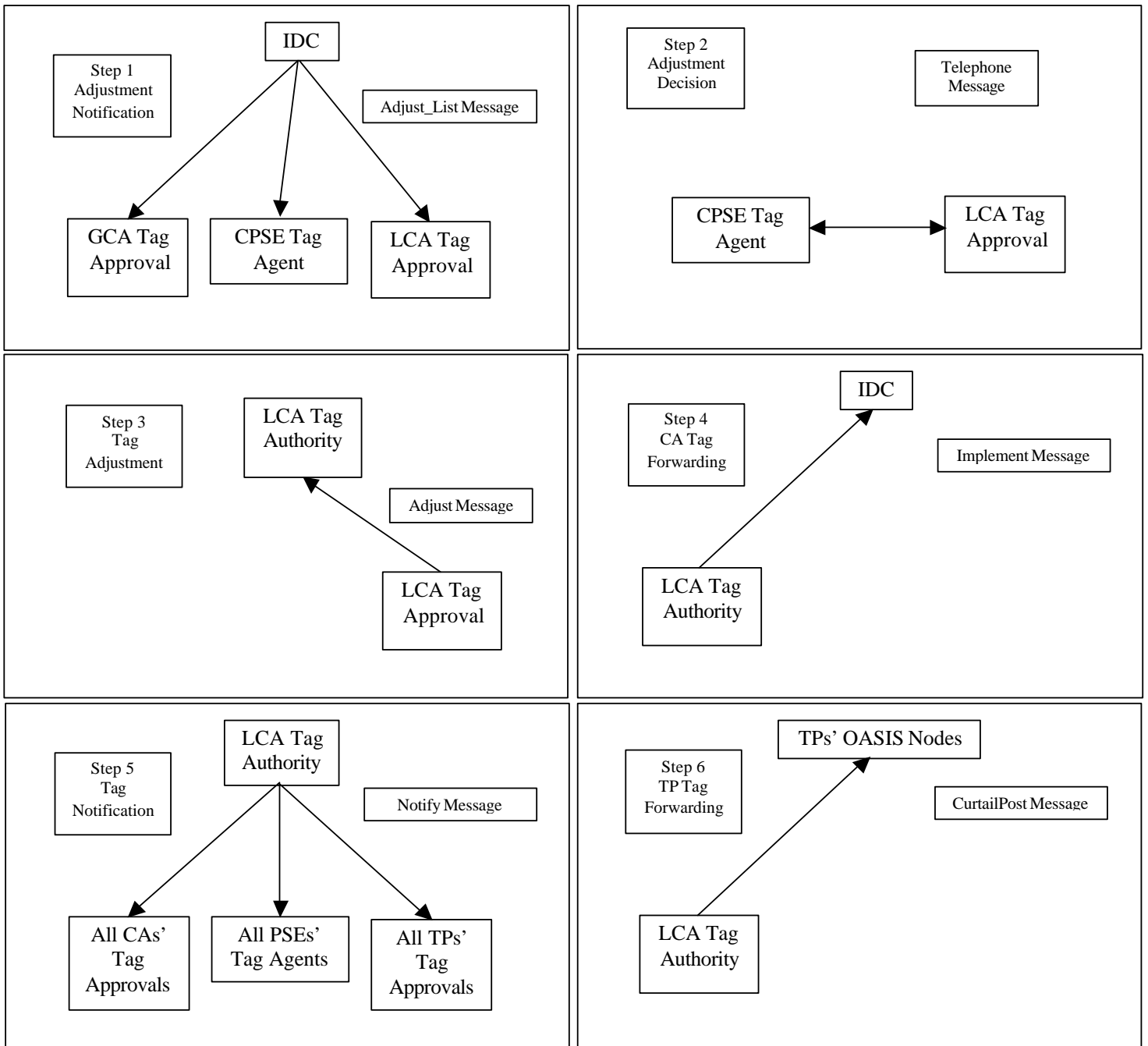
**Step 2 – the Adjustment Decision Step**– occurs no matter where the curtailment originates, whether from NERC's TLR Procedure, WSCC Unscheduled Flow Reduction (NERC Policy 9, Appendix 9C2), ERCOT actions (Appendix 9C3), or local curtailment events. No changes to the 1.66 spec are needed for this.

**Step 3 – the Tag Adjustment Step**– occurs when the Adjust Message for each impacted tag is sent to the LCA Tag Authority. A modification to the ADJUST message is required to fulfill additional information requirements of TP Tag Forwarding in Step 6.

**Step 4 – the CA Tag Forwarding Step**– occurs when the Implement Message is sent on behalf of the LCA to the forward service of the LCA, namely the IDC. No changes to the 1.66 spec are needed for this.

**Step 5 – the Tag Notification Step**– occurs when the LCA Tag Authority notifies all parties to each individual tag of the change in Composite Status to ADJUST. This includes the TPs on the transaction path, whose individual path segmented transmission schedules are impacted by the curtailment. No changes to the 1.66 spec are needed for this.

**Step 6 – the TP Tag Adjust Forwarding Step**– occurs when the CURTAIL\_POST Message is sent on behalf of each TP to the forward service of each TP, namely their OASIS Node. This is optional if the forward service for a TP is not listed. Changes to the E-Tag Functional Specification – 1.66.03 – are needed for this step.



**Figure 2. Tag Adjustment With TP Tag Forwarding**

## 6.1 ADJUST Message Modifications

The primary reason for ADJUST message modification is the need to promulgate non-TLR curtailments to the TPs' tag forward services, namely their OASIS Nodes. For this reason, the following format is proposed to revise the ADJUST message:

```
ADJUST <Target Entity> <Tag ID> <Tag Key>
<Adjust Start Date Time>,<Adjust Stop Date Time>,<MW Cap>,"<Operator ID>","<Reason>",
< Provider_Action>,<Curtailment_Options>,<Event_Id>,<Security_Type>,<Initiating_Party>,<Responsible_Party>,
<Procedure_Name>,<Procedure_Level>,<Facility_Class>,<Facility_Limit_Type>,<Facility_Location>,<Facility_Name>
ADJUST_END
```

*Example:*

```
ADJUST ISNE PJM_PECOENAYA19DH_ISNE LCA1234567890AB
11/12/2000 15:00,11/30/2000 23:00,39,BRUCE_URBSCHAT,"TLR Level 3A on flowgate 9084 at 11/12/2000 14:31:00 (CST)"
CURTAILED,NONE,9084,L,IMO,IMO,TLR,3A,FLOWGATE,THERMAL,EXTERNAL,IMO-MECS
ADJUST_END
```

If the adjustment is valid, then an adjust record is created to represent the adjustment. If there is no ADJUST table present, it is created; otherwise, the record is appended to the existing ADJUST table. The adjust record is populated as follows:

Adjust Date Time	<the current date and time>
Start Date Time	<the start date and time specified in the ADJUST message>
Stop Date Time	<the stop date and time specified in the ADJUST message>
Megawatt Cap	<the megawatt Cap specified in the ADJUST message>
Entity Type	<set to the entity type of the entity issuing the ADJUST request>
Entity Code	<the registered NERC acronym of the entity issuing the ADJUST request>
Operator ID	<the identifier associated with the user that issued the ADJUST request>
Reason	<the REASON for the adjustment, as specified in the ADJUST request>
Provider_Action	< PROVIDER_ACTION indicates the particular action taken by the Transmission Provider with respect to the scheduled transaction; specific values to be returned are, DENIED if the schedule was not started as requested, CURTAILED if the scheduled MW was limited for reliability reasons, or INTERRUPTED if the scheduled MW was limited for economic reasons.> 1{ALPHANUMERIC}25
Curtailment_Options	< Customer options, if any, to avoid curtailment>0{ALPHANUMERIC}80
Event_Id	<The EVENT_ID Data Element is any regional or interconnection-wide recognized security event identifier for events that are of greater scope than those administered locally by the Provider (e.g., a NERC Security Coordinator assigned identifier corresponding to a particular implementation of the NERC TLR procedure). EVENT_ID + PROCEDURE_NAME must be unique.>0{ALPHANUMERIC}25
Security_Type	< SECURITY_TYPE identifies the type of information posted for the event; restricted values are OUTAGE for postings reflecting the state of critical transmission facilities, and LIMIT for postings reflecting the implementation of security procedures to limit or reduce scheduled transactions.> 1{ALPHANUMERIC}
Initiating_Party	< Person's name or Company code for company responsible for initiating the change in capacity>0{ALPHANUMERIC}4
Responsible_Party	<The company code or the name of the person who initiated the reduction, e.g. the security coordinator code>1{ALPHANUMERIC}25
Procedure_Name	< NERC, USF or local procedure name Example: TLR, USF> 1{ALPHANUMERIC}25
Procedure_Level	< NERC, WSCC or local procedure level Example: 2a, 3> 1{ALPHANUMERIC}25
Facility_Class	Type of limiting device such as 'transformer', 'line' or 'flowgate' 1{ALPHANUMERIC}25
Facility_Limit_Type	<For example: thermal, stability, voltage>1{ALPHANUMERIC}25
Facility_Location	<Location of facility that caused the interruption, either internal to the TP or external to the TP grid>1{ALPHANUMERIC}25
Facility_Name	< Name of facility, such as name of path or name of flowgate> 1{ALPHANUMERIC}25

## 6.2 The CURTAIL\_POST Message or curtailpost template CSV Upload

### 6.2.1 Usage

Used by the LCA Tag Authority to submit curtailment details to OASIS Nodes of schedules that have been adjusted under a security event or for some other reason. This message is unique in that it contains the OASIS How WG -published Input Template, curtailpost, for CSV Upload (See Section 2 above).

There are two approaches to implementation of TP Tag Adjust Forwarding:

1. CURTAIL\_POST TMP Message for Indirect Data Delivery of CSV Upload file for OASIS curtailpost template. This assumes an E-Tag System Data Service resides on the OASIS Node.
2. Direct CSV Upload using curtailpost template. No E-Tag Data Service is required.

There are different security requirements depending on the implementation mentioned above.

1. Indirect Data Delivery of CSV Upload file for curtailpost template. If an E-Tag System Data Service resides on the OASIS Node, then the "Authentication Key" field must specify a randomly generated key to be assigned to the recipient of the message. The "Authentication Key" field must comply with the general format for a Tag Key (entity code plus 12 character unique security token). The Entity Code to be used in creating the key shall be the TP code.
2. Direct CSV Upload using curtailpost template. If a TP provider certificate or basic authentication (username:Password) is supplied to the LCA's Tag Authority, then the Tag Authority could login after establishing a connection to the TP forwarding service URL and proceed with a direct curtailpost CSV upload without applying the TMP message wrapper.

When using the CURTAIL\_POST message, the message contents should contain the curtailpost template for upload on OASIS. The information to build the template is supplied from the modified ADJUST Table.

```
CURTAIL_POST <Target Entity> <Authentication Key>
<curtailpost template data>
CURTAIL_POST_END
```

*Example:*

```
CURTAIL_POST NRTG NRTG1234567890AB
VERSION=1.4
TEMPLATE=curtailpost
OUTPUT_FORMAT=DATA
PRIMARY_PROVIDER_CODE=
PRIMARY_PROVIDER_DUNS=
RETURN_TZ=CS
DATA_ROWS=1
COLUMN_HEADERS=PROVIDER_ACTION,SCHEDULE_LIMIT,CURTAILMENT_OPTIONS,ASSIGNMENT_REF,
TRANSACTION_ID,SECURITY_REF,START_TIME,STOP_TIME,EVENT_ID,SECURITY_TYPE,INITIATING_PARTY,
RESPONSIBLE_PARTY,PROCEDURE_NAME,PROCEDURE_LEVEL,FACILITY_CLASS,FACILITY_LIMIT_TYPE,
FACILITY_LOCATION,FACILITY_NAME
CURTAILED, 39,NONE,29345, PJM_PECOENAYA19DH_ISNE,,11/12/2000 15:00,11/30/2000 23:00,9084,L,IMO,IMO,TLR,3A,
FLOWGATE,THERMAL,EXTERNAL,IMO-MECS
CURTAIL_POST_END
```

Upon an LCA's request to post the adjustment of a tag to all TPs' OASIS Nodes, for each TP, the Tag Authority Service must first determine the TP Forwarding Service and method for the transmission provider.

If the Method is TMP the CURTAIL\_POST Message is sent to the TP Forwarding URL after establishing a connection following the TMP protocol. The Data Service at the OASIS Node can provide the final result as a csv file for upload or can insert the received data directly into the OASIS through a back-end process. Alternatively, after the Data Service has transferred the data and removed the message wrapper, a separate process can retrieve the unwrapped csv file and insert the data to OASIS through a call-level interface.

If the Method is OASIS, the TP forwarding service should be set to the TP's OASIS Home directory: "http://(oasis node name):Port/OASIS/Primary\_Provider\_Code. Examples of OASIS message passing are given below.

- ?? **For a JTSIN OASIS Node, on Submit:** action= http://nepooldev.jtsin.com:488/OASIS/NRTG/data/upload method=post  
<csv file to be uploaded>
- ?? **For a JTSIN OASIS Node using TradeAgent's API with Post Method:**  
>C:\taapi -H -L Certificate Filename,Password -T 127.0.0.1:8488 -S <Escaped data to  
be POSTed> "http://nepooldev.jtsin.com:488/OASIS/NRTG/data/upload
- ?? **For a JTSIN OASIS Node using TradeAgent's API with Get Method:**  
>C:\taapi -H -L Certificate Filename,Password -T 127.0.0.1:8488  
"http://nepooldev.jtsin.com:488/OASIS/NRTG/data/curtailpost?version=1.4&etc
- ?? **For an OASIS Node using basic authentication with Get Method:**  
"http://Username:Password@oasis.mepcots.com/oasis/mepc/html/curtailpost?version=1.4&e