DATE:       June 2, 2011

FROM:       E-RSC Working Group

TO:         Gregory Camet
            Kimberly Despeaux
            John Hurstull
            Mark McCulla
            Erin Murphy

SUBJ:       Request for Information No. 12

The E-RSC Working Group has identified the following questions or action items for
your immediate attention. Please provide us this information by 4:00 CDT on June
17, 2011. If you have any clarifying questions or would like to discuss the timelines
provided, please contact Sam Loudenslager, at 501-682-5824 or via email at
sloudenslager@psc.state.ar.us.

- Attached is SPP’s draft classification of data based on their view of
  sensitivity and need for data protection. SPP continues to review this
  listing and may make changes to the document as they move forward
  with their members. As a starting point, the E-RSC Working Group
  would like Entergy to review this listing and for any classification that
  Entergy would disagree with the SPP treatment, please provide an
  explanation of why Entergy views the classification differently.

Please provide responses by the dates provided above by sending the response by
email to: ERSCWorkingGroup@SPP.org.

The ERSC WG expects that responses to this request will be accurate and complete.
To the extent that you believe additional information or data is required to ensure
an accurate response, you have an obligation to timely identify and provide that
information or data in good faith.

The E-RSC Working Group will be requesting additional information in the coming
weeks and in the meantime, appreciates your assistance by providing the
information and in the timeframe requested.
Southwest Power Pool, Inc.
Information Classification

**SPP Restricted**

“SPP Restricted” means any material designated by SPP to be shared with all or a subset of SPP members, transmission customers, and/or market participants.

**Examples of SPP Restricted information include, but are not limited to:**

1. Market settlement information;
2. Certain network configuration required to enable the conduct of business;
3. Certain legal opinions issued;
4. Certain studies;
5. Operating situational reports;
6. Customer daily settlement statements;
7. General Settlements communications (including disputes and resolutions, general communications with customer);
8. Market dispute data;
9. Customer accounts;
10. Code of Conduct Agreement;
11. Engineering project tracking (including Notice to Construct, Engineering and Construction Schedule, Transmission Upgrade Costs, Unintended Consequences);
12. ITO project documentation (including PRPC requests, status updates, scope documents);
13. Daily Operations Reliability reports;
14. Market settlement transaction data;
15. Transmission settlement transaction data;
16. Generation Interconnect studies (including feasibility studies, impact studies, facilities studies);
17. Current/Next Day Studies; and
18. 729 AFC calculation data.

**SPP Confidential**

“SPP Confidential” means any material designated by SPP, its member(s), vendor(s), customer(s), or SPP market participant(s) as “confidential”. The material is for internal SPP use only and cannot be released outside of SPP without executive approval and/or a non-disclosure agreement. Improper disclosure of SPP Confidential information may result in a business disadvantage or a breach of SPP’s contractual obligations. SPP Confidential information may be restricted to a defined subset of SPP employees.
Examples of SPP Confidential information include, but are not limited to:

1. HR records;
2. Contracts;
3. Compliance records related specifically to SPP;
4. Application system specifications;
5. Operating procedures;
6. Certain studies;
7. Board member annual compensation fee and expense reimbursement;
8. Board member expense reports;
9. Employee expense reports;
10. Invoices for goods and services received by SPP;
11. Invoices for shared services (including Regional Entity and ISO-RTO Council shared expenses borne by another entity);
12. Manually processed expenses (including prospective employee interview, tuition reimbursement, relocation);
13. Regional Entity Trustee expense reports;
14. Relocation moving expenses paid to vendor;
15. Relocation reimbursement (travel, lodging, meals) paid to employee;
16. Customer/member credit memos;
17. Customer receipts (including payments for training classes, system maps);
18. Invoices for goods and services provided by SPP;
19. Return credit/refunds;
20. Tariff and Market invoices;
21. Actuarial Report;
22. Benefits statements (including 401K plan, Defined Benefit Plan, retirement information);
23. Bank statements (including deposit/withdrawal records, reconciliation);
24. Check stubs (including bank statement images);
25. Department budget submission;
26. Monthly budget forecast submission;
27. Monthly budget reports;
28. Monthly SPP-RE expenses report;
29. Credit files (including financial statements, credit reviews);
30. Employee credit card requests;
31. Facilities asset list;
32. Non-IT capital assets documentation;
33. General ledger;
34. Child support, levies;
35. Garnishments;
36. Cafeteria plan and benefits, 401k, supplemental insurance, United Way;
37. Payroll general ledger entries, accruals, taxes;
38. Purchase orders (including supporting documentation);
39. Requisitions (including supporting documentation);
40. Requests for Information/Proposal (including supporting documents such as evaluation team documents and recommendations);
41. Market settlement validation;
42. Transmission settlement validation;
43. Audit response to SAS-70 audits;
44. Market participant audit;
45. SAS-70 Audit;
46. Auditor’s report, management letter;
47. Pension Plan audit;
48. Risk matrix (Management risk assessment);
49. Internal audit documentation (audit report details and supporting documentation, summary of audits completed, recommendations, interim reports, management response);
50. Business plans for services provided to members;
51. Contract services agreements;
52. Contract services contracts (ICT, ITO, others);
53. Credit and Security Agreement (guarantee agreement, letters of credit);
54. Non-disclosure agreements (contracts, vendors, consultants, annual member NDA);
55. Software licenses;
56. Stakeholder communications between the ICT and the customer;
57. Board member compensation notification letters;
58. HR-related legal correspondence;
59. Contract-related market complaints (participant complaints, participant inquiries, PUC/PSC/Corporate Commission inquiry);
60. FERC-related market complaints (participant complaints, participant inquiries, PUC/PSC/Corporate Commission Inquiry);
61. Generation Interconnection Customer accounts (master list of accounts);
62. Applications for OASIS access;
63. Customer registration packet (billing information, contacts, financial information, LSA designation, routing information);
64. Market registration (includes company basic information, resource information, settlement locations, meter agent designations);
65. Departmental business continuity plans;
66. Backup (disaster recovery) site procedure;
67. Equipment maintenance/inspection reports (including generator, UPS, fire protection, electrical infrastructure, HVAC);
68. Building plans (architectural drawings, floor plans, construction plans, as-builts) that do not contain information to be protected per the NERC reliability standards (includes plans submitted to the jurisdictional planning and zoning commissions);
69. HR reports (including benefit plan financial status (5500), EEO, New hire report, H-1B, IRS W-3);
70. Federal employer returns, quarterly, annual;
71. Market monitor filings;
72. Employee payroll file (including W-4, personnel change requests, benefits change forms, deduction authorizations);
73. Payroll information (salary, promotion documentation, merit/bonus, personnel action forms);
74. Employee performance reviews;
75. Organization chart;
76. Personnel risk assessment documentation (employee, vendor, contractor);
77. On-call list;
78. Billable time reports;
79. Time and attendance reporting;
80. Insurance claims (including accident reports, claims filing, settlements, supporting documentation);
81. Insurance enrollment forms;
82. Business insurance policies (including general liability, negligence, property, casualty, umbrella liability, errors and omissions);
83. Group disability (short-term disability, long-term disability);
84. Insurance policy documents;
85. Accident reports (including Worker’s Comp);
86. Fire inspection reports;
87. Internal SPP meeting minutes (departmental, management team, etc.);
88. Regional Entity financial report to NERC;
89. ICT Operations logs;
90. ITO Operations logs;
91. Forecast Offset logs;
92. MISO call logs;
93. SERC call logs;
94. Shift engineer logs;
95. Reliability logs;
96. RSS issues logs;
97. Time error correction logs;
98. NERC Reliability Standards compliance policies and procedures;
99. ITO operating procedures;
100. WPP policies and procedures (including WPP procedure manual, software technical documentation, test plans);
101. Corporate procedures;
102. Facility use (facility use policies, training room policies, audiovisual equipment use instructions);
103. Business process controls (SAS-70 controls, NERC Reliability Standard compliance controls);
104. Departmental process and procedure documentation, process maps, process narratives;
105. Project Management documentation other than the Project Management workbook;
106. Project plans and other project artifacts not under Project Management Office control;
107. Project Portfolio (non-public content including project portfolio, project requests, prioritization and ranking schedules, metrics reports, PRPC status reports);
108. Destruction approvals, confirmations of destruction;
109. Annual Report supporting materials;
110. Market settlement internal reports;
111. Visitor logs (temporary escorted/unescorted visitor badge issuance, temporary employee badge issuance, training room badge issuance);
112. HR reports (including Worker’s Comp);
113. State quarterly/annual employer returns;
114. ICT Transmission planning studies (unredacted);
115. ITO transmission planning studies (including NITS, system impact/long-term transmission studies, transmission expansion plans);
116. Internal surveys – employee;
117. Training records (including attendance rosters, exam results, class evaluations, course transcripts, NERC Certification Numbers);
118. Comprehensive training course materials;
119. Job task assessment;
120. Training plans (including strategic training plan, yearly training plan);
121. Class roster (including formal training attendance records, informal training attendance records);
122. Operating day data;
123. Transmission reservation data;
124. Transmission schedule data; and
125. Operating day studies and modeling data.

**SPP Highly Sensitive**

“SPP Highly Sensitive” means any material designated by SPP, its member(s), vendor(s), customer(s), or SPP market participant(s) as “CEII”, “highly sensitive”, “protected”, “proprietary”, or other such designation as indicates protection of the material, and includes any material so designated by SPP, its member(s), vendor(s), customer(s), or SPP market participant(s) that was provided to SPP by another party where the other party claims such material to be competitively sensitive, commercial or financial information, or trade secret information. SPP Highly Sensitive information is highly confidential and, if improperly released, could potentially result in harm to the nation’s critical infrastructure.

Included in the “SPP Highly Sensitive” classification is material that meets FERC’s definition of Critical Energy Infrastructure Information (CEII). CEII is defined by the regulations of the Federal Energy Regulatory Commission.
(“FERC”) at 18 C.F.R. § 388.113(c)(1) as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure\(^1\) that:

(i) Relates details about the production, generation, transportation, transmission, or distribution of energy;
(ii) Could be useful to a person in planning an attack on critical infrastructure;
(iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
(iv) Does not simply give the general location of the critical infrastructure.

Also included in the “SPP Highly Sensitive” classification is information subject to the access control requirements of North American Electric Reliability Corporation Reliability Standard CIP-003-3 (Cyber Security – Security Management Controls), Requirement R4 (Information Protection).

**Examples of SPP Highly Sensitive information include, but are not limited to:**

1. SPP power flow base case data (submitted as Part 2 of FERC Form No. 715);
2. The SPP Transmission Map (submitted as Part 3 of FERC Form No. 715);
3. The SPP Transmission Expansion Plan (“STEP”) Map;
4. The SPP Transmission Atlas;
5. SPP Model Development Working Group reduced models and stability models;
6. Aggregate Transmission Service Study models;
7. Generation Interconnection models;
8. STEP models;
9. Ventyx models;
10. Offers from the Market;
11. Unit commitment stack used in planning and operations;
12. Critical Asset and Critical Cyber Asset lists;
13. Network topology or similar diagrams;
14. Floor plans of computing centers that contain Critical Cyber Assets;
15. Equipment layouts of Critical Cyber Assets;
16. Disaster recovery plans;
17. Incident response plans;

\(^1\) Critical infrastructure means existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters. 18 C.F.R. § 388.113(c)(2).
18. Security configuration information such as user names, passwords, IP addresses, and firewall rules;
19. IT asset documentation (hardware inventory, software inventory);
20. Audit responses to NERC audits;
21. Audit responses to NERC readiness assessments;
22. Audit responses to SERC audits;
23. NERC Compliance Audits;
24. NERC Readiness Evaluations;
25. NERC Reliability Standards compliance audit artifacts;
26. SERC Compliance Audits;
27. Audit responses to FERC audits, GAO audits, and other non-NERC regulatory audits;
28. FERC audits, GAO audits, other non-NERC regulatory audits;
29. Corporate emergency response plans;
30. Entity blackstart plans;
31. Operating plans (includes Emergency Plan, Reliability Plan);
32. Regional blackstart plan, regional restoration plan;
33. Facility technical designs (data center layout, environmental systems, coordination center layout);
34. EIA-411 Report (full version);
35. Data requests, notices, other NERC filings;
36. Reliability standards compliance (including compliance self-certification);
37. Application support procedures (including run books, installation/removal procedures, configuration procedures, checklists, change processes);
38. Database support procedures (including start-up, shutdown, fail over, backup, restoration);
39. Operating guides;
40. Operating procedures;
41. Project Management workbooks (including project artifacts);
42. Access documentation (employee physical access requests, visitor physical access requests, cyber access requests other than database);
43. Database access requests;
44. Digital certificate requests;
45. Security architecture (physical security perimeter design, electronic security perimeter design, security plans);
46. Security policy exceptions (approved/denied company security policy exception requests, NERC CIP compliance technical feasibility exceptions);
47. Reportable security incidents; and