

**BEFORE THE
PUBLIC UTILITIES COMMISSION OF OHIO**

THE DAYTON POWER AND LIGHT COMPANY

CASE NO. 15-1830-EL-AIR

CASE NO. 15-1831-EL-AAM

CASE NO. 15-1832-EL-ATA

2015 DISTRIBUTION BASE RATE CASE

**BOOK I – APPLICATION AND SUPPLEMENTAL
VOLUME 3 OF 14**

This is to certify that the images appearing are an
accurate and complete reproduction of a case file
document delivered in the regular course of business.
Technician ML Date Processed NOV 30 2015

RECEIVED

NOV 30 2015

Dayton Power and Light Company
DP&L Case No. 15-1830-EL-AIR
Standard Filing Requirements for Rate Increases
Table of Contents

DOCKETING DIVISION
Public Utilities Commission of Ohio

| Book # | Vol # | OAC 4901-7-01 Reference | Schedule | Description |
|--|-------|--|--------------|---|
| OAC 4901-7 | | | | |
| Appendix A, Chapter II, (B) Supplemental Filing Requirements | | | | |
| 1 | 1 | Appendix A, Chapter II, (B)(1)(a)-(f) | S-1 | Most recent 5 year capital expenditures budget. |
| 1 | 1 | Appendix A, Chapter II, (B)(2)(a)-(c) Appendix A, Chapter II, (B)(3)(a)-(d) | S-2 | Most recent 5 year financial forecast and support for the underlying assumptions. |
| 1 | 1 | Appendix A, Chapter II, (B)(7) | S-3 | A proposed notice for newspaper publication. |
| 1 | 1 | Appendix A, Chapter II, (B)(8) | S-4.1 | An executive summary of applicant utility's corporate process. |
| 1 | 2-3 | Appendix A, Chapter II, (B)(9) | S-4.2 | An executive summary of applicant utility's management policies, practices, and organization. |
| OAC 4901-7 | | | | |
| Appendix A, Chapter II, (C) Supplemental Information Provided at Filing | | | | |
| 1 | 3 | Appendix A, Chapter II, (C)(1) | Supplemental | The most recent Federal Energy Regulatory Commission's ("FERC") audit report. |
| 1 | 3 | Appendix A, Chapter II, (C)(2) | Supplemental | Prospectuses of current stock and/or bond offering of the applicant, and/or of parent company. |
| 1 | 4-8 | Appendix A, Chapter II, (C)(3) | Supplemental | Annual reports to shareholders of the applicant, and/or parent company for the most recent five years and the most recent statistical supplement. |
| 1 | 9-12 | Appendix A, Chapter II, (C)(4) | Supplemental | The most recent SEC Form 10-K, 10-Q, and 8-K of the applicant, and/or parent company. |
| 1 | 13 | Appendix A, Chapter II, (C)(5) | Supplemental | Working papers supporting the schedules. |
| 1 | 14 | Appendix A, Chapter II, (C)(6) | Supplemental | Worksheet showing monthly test year data by FERC account. |
| 1 | 14 | Appendix A, Chapter II, (C)(7) | Supplemental | CWIP included in the prior case. |
| 1 | 14 | Appendix A, Chapter II, (C)(8) | Supplemental | Copy of latest certificate of valuation from department of taxation. |
| 1 | 14 | Appendix A, Chapter II, (C)(9) | Supplemental | Monthly sales for the test year by rate schedule classification and/or customer classes. |
| 1 | 14 | Appendix A, Chapter II, (C)(10) | Supplemental | Written summary explaining the forecasting method used by the utility as related to test year data. |
| 1 | 14 | Appendix A, Chapter II, (C)(11) | Supplemental | Explanation of computation of materials and supplies. |
| 1 | 14 | Appendix A, Chapter II, (C)(12) | Supplemental | Depreciation expense related to specific plant accounts. |
| 1 | 14 | Appendix A, Chapter II, (C)(13) | Supplemental | Federal income tax information. |
| 1 | 14 | Appendix A, Chapter II, (C)(14) | Supplemental | Other rate base items and detailed information. |
| 1 | 14 | Appendix A, Chapter II, (C)(15) | Supplemental | Copy of all advertisements in the test year. |
| 1 | 14 | Appendix A, Chapter II, (C)(16) | Supplemental | Plant in service data from the last date certain to the date certain in the current case. |
| 1 | 14 | Appendix A, Chapter II, (C)(17) | Supplemental | Depreciation study showing depreciation reserves allocated to accounts. |
| 1 | 14 | Appendix A, Chapter II, (C)(18) | Supplemental | Depreciation study. |
| 1 | 14 | Appendix A, Chapter II, (C)(19) | Supplemental | Depreciation reserve data from the last date certain to the date certain in the current case. |
| 1 | 14 | Appendix A, Chapter II, (C)(20) | Supplemental | Construction project details for projects that are at least seventy-five percent complete. |
| 1 | 14 | Appendix A, Chapter II, (C)(21) | Supplemental | Surviving dollars by vintage year of placement (original cost data as of date certain for each individual plant account). |
| 1 | 14 | Appendix A, Chapter II, (C)(22) | Supplemental | Test year and two most recent calendar years' employee levels by month. |

Dayton Power and Light Company
DP&L Case No. 15-1830-EL-AIR
Standard Filing Requirements for Rate Increases
Table of Contents

| Book # | Vol # | OAC 4901-7-01 Reference | Schedule | Description |
|--|-------|---|----------|--|
| OAC 4901-7 | | | | |
| Appendix A, Chapter II, Section A | | | | |
| 2 | 1 | Appendix A, Chapter II, Section A(B) | A-1 | Overall Financial Summary |
| 2 | 1 | Appendix A, Chapter II, Section A(C) | A-2 | Computation of Gross Revenue Conversion Factor |
| 2 | 1 | Appendix A, Chapter II, Section A(D) | A-3 | Calculation of Mirrored CWIP Revenue Sur-Credit Rider |
| OAC 4901-7 | | | | |
| Appendix A, Chapter II, Section B | | | | |
| 2 | 1 | Appendix A, Chapter II, Section B(B)(1) | B-1 | Jurisdictional Rate Base Summary |
| 2 | 1 | Appendix A, Chapter II, Section B(B)(2) | B-2 | Plant in Service Summary by Major Property Groupings |
| 2 | 1 | Appendix A, Chapter II, Section B(B)(3) | B-2.1 | Plant in Service By Accounts & Subaccounts |
| 2 | 1 | Appendix A, Chapter II, Section B(B)(4) | B-2.2 | Adjustments to Plant in Service |
| 2 | 1 | Appendix A, Chapter II, Section B(B)(5) | B-2.3 | Gross Additions, Retirements and Transfers |
| 2 | 1 | Appendix A, Chapter II, Section B(B)(6) | B-2.4 | Lease Property |
| 2 | 1 | Appendix A, Chapter II, Section B(B)(7) | B-2.5 | Property Excluded from Rate Base |
| 2 | 1 | Appendix A, Chapter II, Section B(C)(1) | B-3 | Reserve for Accumulated Depreciation |
| 2 | 1 | Appendix A, Chapter II, Section B(C)(2) | B-3.1 | Adjustments to the Reserve for Accumulated Depreciation |
| 2 | 1 | Appendix A, Chapter II, Section B(C)(3) | B-3.2 | Depreciation Accrual Rates and Jurisdictional Reserve Balances by Accounts |
| 2 | 1 | Appendix A, Chapter II, Section B(C)(4) | B-3.3 | Depreciation Reserve Accruals, Retirements and Transfers |
| 2 | 1 | Appendix A, Chapter II, Section B(C)(5) | B-3.4 | Depreciation Reserve and Expense for Lease Property |
| 2 | 1 | Appendix A, Chapter II, Section B(D)(1) | B-4 | Construction Work in Progress ("CWIP") |
| 2 | 1 | Appendix A, Chapter II, Section B(D)(2) | B-4.1 | CWIP Percent Completed - Time |
| 2 | 1 | Appendix A, Chapter II, Section B(D)(3) | B-4.2 | CWIP Percent Completed - Dollars |
| 2 | 1 | Appendix A, Chapter II, Section B(E)(1) | B-5 | Allowance for Working Capital |
| 2 | 1 | Appendix A, Chapter II, Section B(E)(2) | B-5.1 | Miscellaneous Working Capital Items |
| 2 | 1 | Appendix A, Chapter II, Section B(F)(1) | B-6 | Other Rate Base Items Summary |
| 2 | 1 | Appendix A, Chapter II, Section B(F)(2) | B-6.1 | Adjustments to Other Rate Base Items |
| 2 | 1 | Appendix A, Chapter II, Section B(F)(3) | B-6.2 | Contributions in Aid of Construction ("CIAC") by Accounts and Subaccounts |
| 2 | 1 | Appendix A, Chapter II, Section B(G)(1) | B-7 | Jurisdictional Allocation Factors |
| 2 | 1 | Appendix A, Chapter II, Section B(G)(2) | B-7.1 | Jurisdictional Allocation Statistics |
| 2 | 1 | Appendix A, Chapter II, Section B(G)(3) | B-7.2 | Explanation of Changes in Allocation Procedures |
| 2 | 1 | Appendix A, Chapter II, Section B(I) | B-9 | Mirrored CWIP Allowances |

Dayton Power and Light Company
DP&L Case No. 15-1830-EL-AIR
Standard Filing Requirements for Rate Increases
Table of Contents

| Book # | Vol # | OAC 4901-7-01 Reference | Schedule | Description |
|--|-------|--|----------------------|--|
| OAC 4901-7 | | | | |
| Appendix A, Chapter II, Section C | | | | |
| 2 | 1 | Appendix A, Chapter II, Section C(B)(1) | C-1 | Jurisdictional Proforma Income Statement |
| 2 | 1 | Appendix A, Chapter II, Section C(B)(2) | C-2 | Adjusted Test Year Operating Income |
| 2 | 1 | Appendix A, Chapter II, Section C(B)(3) | C-2.1 | Operating Revenues and Expenses by Account - Jurisdictional Allocation |
| 2 | 1 | Appendix A, Chapter II, Section C(C)(1) | C-3 | Summary of Jurisdictional Adjustments to Operating Income |
| 2 | 1 | Appendix A, Chapter II, Section C(C)(2) | C-3.1 through C-3.25 | Jurisdictional Adjustments to Operating Income |
| 2 | 1 | Appendix A, Chapter II, Section C(D)(1) | C-4 | Adjusted Jurisdictional Income Taxes |
| 2 | 1 | Appendix A, Chapter II, Section C(D)(2) | C-4.1 | Development of Jurisdictional Income Taxes Before Adjustments |
| 2 | 1 | Appendix A, Chapter II, Section C(D)(3)(a) | C-5 | Social and service club dues |
| 2 | 1 | Appendix A, Chapter II, Section C(D)(3)(b) | C-6 | Charitable Contributions |
| 2 | 1 | Appendix A, Chapter II, Section C(D)(4) | C-7 | Customer Service and Informational, Sales and Miscellaneous Advertising Expense or Marketing Expense |
| 2 | 1 | Appendix A, Chapter II, Section C(D)(5) | C-8 | Rate Case Expense |
| 2 | 1 | Appendix A, Chapter II, Section C(D)(6) | C-9 | Operation and Maintenance Payroll Cost |
| 2 | 1 | Appendix A, Chapter II, Section C(D)(7) | C-9.1 | Total Company Payroll Analysis by Employee Classification/Payroll Distribution |
| 2 | 1 | Appendix A, Chapter II, Section C(E)(1) | C-10.1 | Comparative Balance Sheets for the Most Recent Five Calendar Years |
| 2 | 1 | Appendix A, Chapter II, Section C(E)(2) | C-10.2 | Comparative Income Statements for the Most Recent Five Calendar Years |
| 2 | 1 | Appendix A, Chapter II, Section C(E)(3) | C-11.1 | Revenue Statistics - Total Company |
| 2 | 1 | Appendix A, Chapter II, Section C(E)(3) | C-11.2 | Revenue Statistics - Jurisdictional |
| 2 | 1 | Appendix A, Chapter II, Section C(E)(3) | C-11.3 | Sales Statistics - Total Company |
| 2 | 1 | Appendix A, Chapter II, Section C(E)(3) | C-11.4 | Sales Statistics - Jurisdictional |
| 2 | 1 | Appendix A, Chapter II, Section C(E)(4) | C-12 | Analysis of Reserve for Uncollectible Accounts |
| OAC 4901-7 | | | | |
| Appendix A, Chapter II, Section D | | | | |
| 2 | 1 | Appendix A, Chapter II, Section D(A) | D-1 | Rate of Return Summary |
| 2 | 1 | Appendix A, Chapter II, Section D(B) | D-1.1 | Parent-Consolidated Common Equity |
| 2 | 1 | Appendix A, Chapter II, Section D(C)(1) | D-2 | Embedded Cost of Short-Term Debt |
| 2 | 1 | Appendix A, Chapter II, Section D(C)(2) | D-3 | Embedded Cost of Long-Term Debt |
| 2 | 1 | Appendix A, Chapter II, Section D(C)(3) | D-4 | Embedded Cost of Preferred Stock |
| 2 | 1 | Appendix A, Chapter II, Section D(D) | D-5 | Comparative Financial Data |

Dayton Power and Light Company
DP&L Case No. 15-1830-EL-AIR
Standard Filing Requirements for Rate Increases
Table of Contents

| Book # | Vol # | OAC 4901-7-01 Reference | Schedule | Description |
|---|-------|--|----------|---|
| OAC 4901-7 Appendix A, Chapter II, Section E | | | | |
| 2 | 2 | Appendix A, Chapter II, Section E(B)(1) | E-1 | Clean Copy of Proposed Tariff Schedules |
| 2 | 3 | Appendix A, Chapter II, Section E(B)(2)(a) | E-2 | Current Tariff Schedules |
| 2 | 4 | Appendix A, Chapter II, Section E(B)(2)(b) | E-2.1 | Redlined Copy of Proposed Tariff Schedules |
| 2 | 1 | Appendix A, Chapter II, Section E(B)(3) | E-3 | Rationale for Tariff Changes |
| 2 | 1 | Appendix A, Chapter II, Section E(B)(4) | E-3.1 | Customer Charge / Minimum Bill Rationale |
| 2 | 1 | Appendix A, Chapter II, Section E(B)(5) | E-3.2 | Cost of Service Study |
| 2 | 1 | Appendix A, Chapter II, Section E(C)(2)(a) | E-4 | Class and Schedule Revenue Summary |
| 2 | 1 | Appendix A, Chapter II, Section E(C)(2)(b) | E-4.1 | Annualized Test Year Revenue at Proposed Rates vs. Most Current Rates |
| 2 | 1 | Appendix A, Chapter II, Section E(D) | E-5 | Typical Bill Comparison |

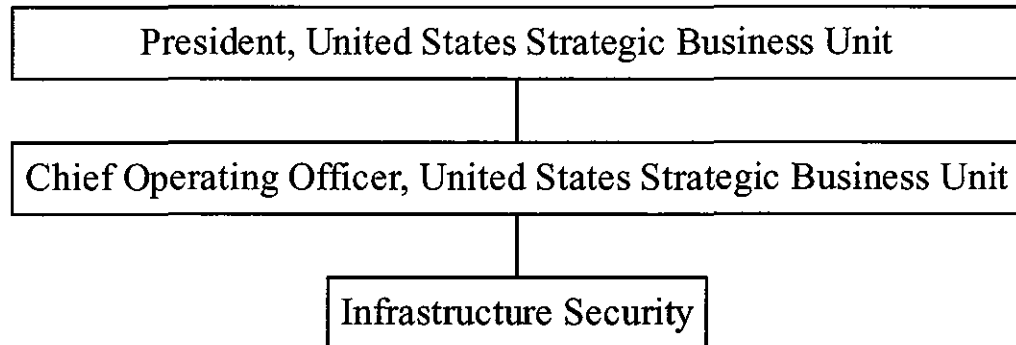
The Dayton Power and Light Company

Executive Summary of Management Policies Practices and Organization

Schedule S-4.2, Part 2

Infrastructure Security

Infrastructure Security has overall responsibility for physical and cyber security activities at all DP&L locations. The Infrastructure Security function is described in detail in the following section.



Functional Area:
Infrastructure Security Services

SFR Reference
(B)(9)(f)(iii) Policies for Protecting Company and Customer Information/Data

Policy and Goal Setting:

Infrastructure Security Services provides cyber-security, physical security and NERC Critical Infrastructure Protection Standards (“NERC CIP”) compliance services for the transmission, distribution, generation and corporate operations of DP&L.

DP&L’s cyber-security, physical security and NERC CIP compliance policies are determined by business need, regulatory compliance, risk assessments and industry best practices. Policies are developed by management under the guidance of AES’s leadership and AES’s board of directors. All parties are equally responsible to ensure that DP&L policies meet or exceed the requirements set forth by all of DP&L’s regulatory and business requirements.

The first priority of all DP&L areas is to ensure the safety of all DP&L employees, contractors, vendors and the public. Infrastructure Security Services personnel and management takes this priority very seriously, and incorporates safety into all aspects of its operations. The safety program focuses on getting everyone involved in safety in order to increase safety awareness and create an injury-free workplace through monthly safety meetings and DP&L’s safety walk program.

Strategic and Long-Range Planning:

Planning in Infrastructure Security Services for physical security, cyber-security and NERC CIP compliance reflects DP&L’s long-term strategy to achieve DP&L’s goal of delivering safe, reliable service and meeting the compliance and reliability targets as well as our customers’ needs.

Infrastructure Security Services determines long-range planning as part of a multi-year budget cycle based on known compliance requirements, system life cycle management, and threats to the company. In addition to operational needs, the planning stage considers budget allowances and staffing needs.

Organizational Structure and Responsibilities:

Infrastructure Security Services consists of approximately 61 staff members and is led by the Director of Infrastructure Security. This area maintains responsibility for the following utility activities:

1. Physical Security services are provided for 170+ locations within DP&L's geographical footprint and include power stations, substations, service centers, corporate offices, communication/microwave tower sites, remote storage yards and personnel security. Activities include:
 - a. Provide 24/7 security guard services for power stations, corporate offices and special assignments
 - b. Utilize 450+ electronic surveillance cameras at substations, service centers, tower sites and office facilities for situational awareness
 - c. Oversee 142 alarm systems across DP&L's geographical footprint. This includes security check-in and check-out protocols for all substations and tower site locations
 - d. Manage all security operations from the security operations center in DP&L's service building
 - e. Supervise incident response, inquiries and investigations related to physical security and access control
2. Cyber-Security services are provided to Information Technology and Customer Operations. Activities include:
 - a. Protect DP&L's computer network users, architecture and data from malicious activity using security methodologies, processes and technologies
 - b. Monitor DP&L's computer network, data center, workstations, electronic field terminals and personnel activity for external and internal threats
 - c. Provide awareness and training programs for DP&L personnel, contractors and vendors
 - d. Identify, classify and protect information assets throughout their lifecycles. DP&L's Information Classification Policy is attached as Security – Exhibit 2.
 - e. Supervise incident response, inquiries and investigations related to cyber-security and data protection
3. NERC CIP regulatory programs enforce mandatory requirements for in-scope business operations at power stations and transmission operation facilities that fall under NERC CIP v3, NERC CIP v5 and NERC CIP 014 compliance standards. A complete listing of the Security Standards is included as Security – Exhibit 3. Activities include:
 - a. Address physical security risks and vulnerabilities related to the reliable operation of DP&L's bulk electric system, including transmission substations
 - b. Provide sabotage incident investigations and regulatory reporting
 - c. Identify and document the critical cyber assets associated with the critical assets that support the reliable operation of DP&L's bulk electric system
 - d. Oversee minimum security management controls to protect DP&L's critical cyber assets according to DP&L's cyber security standards included as Security – Exhibit 4.

- e. Manage DP&L's personnel with authorized cyber or unescorted physical access to DP&L's critical cyber assets, including contractors and service vendors, and ensure DP&L personnel have an appropriate level of personnel risk assessment, training, and security awareness
- f. Manage the identification and protection of DP&L's electronic security perimeters inside which all critical cyber assets reside, as well as all access points on the perimeter
- g. Maintain a physical security program for the protection of DP&L's critical cyber assets
- h. Manage the methods, processes, and procedures for securing DP&L's critical cyber assets, as well as the other (non-critical) cyber assets within DP&L's electronic security perimeters
- i. Ensure the identification, classification, response, and reporting of cyber-security incidents related to DP&L's critical cyber assets
- j. Ensure that recovery plans are put in place for DP&L's critical cyber assets and verify the plans follow established business continuity and disaster recovery techniques and practices

The organizational chart for Infrastructure Security Services is included as Security - Exhibit 1.

Decision-Making and Control:

DP&L's Infrastructure Security Services decision-making and control is achieved by individuals throughout the organization making decisions within their given scope of authority in support of DP&L's overall mission and in accordance with the DP&L policies and procedures. Decisions are raised to a proper level of authority as required by DP&L's policies. Overall responsibility for all Infrastructure Security Services decisions is that of the Director of Infrastructure Security.

Performance against Infrastructure Security Services operational goals is monitored and reported on a continuous basis, which includes monitoring of safety, security operations, budgets, and compliance. This monitoring helps to ensure that early warnings are in place when problems arise. This allows management to uncover trends in a timely manner and proactively address issues.

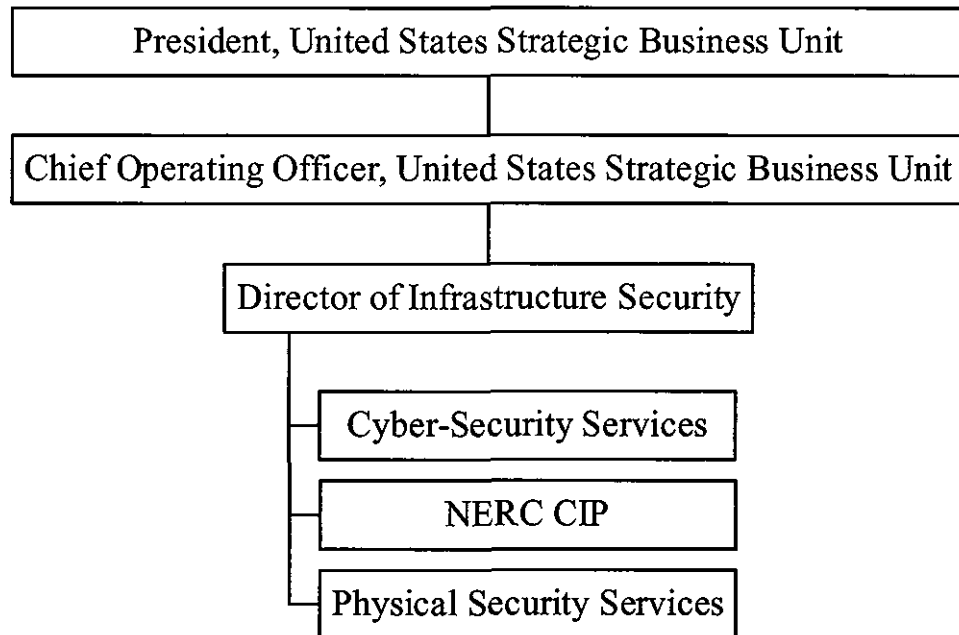
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including: face-to-face meetings, phone calls, conference calls and e-mail. Internal communications typically correspond to supporting the operations of other functional areas of DP&L. These communications include providing information to areas such as the Security Operations Center, Dispatch Operations, Customer Service, Corporate Communications, Finance, and Regulatory Operations.

External communications are accomplished through a variety of communication channels including: phone calls, radio systems, meetings, and e-mail. Infrastructure Security Services personnel and security staff will communicate directly with internal business divisions when incidents or awareness requirements arise. Communications typically involve a variety of topics including: security statuses, incident response, activity alerts, awareness campaigns, and maintenance activities.

Security – Exhibit 1

Organizational chart for Infrastructure Security Services





AES US Strategic Business Unit ("US SBU")

Infrastructure Security Policies

US SBU INFORMATION CLASSIFICATION POLICY

Policy Owner: US SBU Infrastructure Security

Original Issue Date: 02/19/2015

Revision Date: 06/04/2015

US SBU INFORMATION CLASSIFICATION POLICY

Contents

| | | |
|------|---|----|
| 1.0 | INTRODUCTION | 1 |
| 2.0 | SCOPE | 1 |
| 3.0 | PURPOSE | 1 |
| 3.1 | FERC Critical Energy Infrastructure Information (CEII) | 1 |
| 4.0 | DEFINITIONS | 2 |
| 4.1 | Anonymized / Anonymization: | 2 |
| 4.2 | Backup: | 2 |
| 4.3 | Breach of Confidentiality: | 2 |
| 4.4 | Electronic Media: | 2 |
| 4.5 | Encryption / Encrypt: | 2 |
| 4.6 | Encryption Key: | 3 |
| 4.7 | Information Technology (I.T.): | 3 |
| 4.8 | Media: | 3 |
| 4.9 | Mobile Computing Device: | 3 |
| 4.10 | Non-Disclosure (and Confidentiality) Agreement: | 3 |
| 4.11 | Owner: | 3 |
| 4.12 | Personal Identifiable Information – PII (as defined by NIST): | 3 |
| 4.13 | Personal Use: | 3 |
| 4.14 | Pulverize / Pulverized: | 3 |
| 4.15 | Removable Storage Device: | 4 |
| 4.16 | System Owner: | 4 |
| 4.17 | Structured Data: | 4 |
| 4.18 | Unstructured Data: | 4 |
| 4.19 | User: | 4 |
| 5.0 | POLICY | 5 |
| 5.1 | Information Classification | 5 |
| 5.2 | Public/Unclassified Information | 5 |
| 5.3 | Internal Information | 5 |
| 5.4 | Confidential or Restricted Information | 6 |
| 5.5 | Protective Markings | 6 |
| 5.6 | Disclosing Information | 7 |
| 5.7 | Reporting Improper Disclosure or Loss | 7 |
| 5.8 | Example Matrix | 8 |
| 5.9 | Safeguarding and Handling of Information | 9 |
| 5.10 | Disposal and Asset Reuse | 9 |
| 6.0 | CONFLICTS | 9 |
| 7.0 | POLICY ENFORCEMENT | 9 |
| 8.0 | POLICY EXCEPTIONS | 10 |
| 9.0 | STANDARDS AND GUIDELINES | 10 |
| 10.0 | APPROVALS | 10 |
| 11.0 | Version Control History | 11 |
| 12.0 | Appendix A: Information Classification and Handling Matrix | 12 |

**AES US SBU
Policies**

Document Control No.: **IS-010**
Last Revised Date: **6-4-2015**
Page **1**

US SBU INFORMATION CLASSIFICATION POLICY

1.0 INTRODUCTION

The AES Corporation's United States Strategic Business Unit (US SBU) creates, collects and processes a vast amount of information in multiple formats. In addition, the US SBU possesses information concerning our customers identifiable information and information that if misused could be used in the planning or disruption of or to the Bulk Electric System. The US SBU has a responsibility to protect this information and ensure the confidentiality, integrity and availability of data. The US SBU is committed to the correct and proper classification and handling of this information. This policy has been developed to direct personnel in applying a degree of sensitivity and criticality to all the information created, collected, processed and disseminated within and outside the organization.

2.0 SCOPE

This policy is applicable to AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, and any affiliate of US Services that adopts this policy pursuant to its own corporate governance procedures (collectively, the "Companies"). Documentation of adoption of this policy by a US Services affiliate shall be kept by the US Services Policy Committee or it's designate. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp. However, at no time shall this policy conflict with any additional obligations an individual business may have in place to support other requirements, (e.g. NERC CIP). This policy is intended to create a minimum baseline for all US SBU locations and personnel.

3.0 PURPOSE

The purpose of this policy is to ensure information assets are identified, properly classified, and protected throughout their lifecycles. Information, like other assets, must be properly managed from its creation to disposal. As with other assets, not all information has the same value or importance and therefore information requires different levels of protection. Information asset classification and data management are critical to ensure that the assets have a level of protection corresponding to the sensitivity and value of the information asset. This policy collectively applies to all information assets, including but not limited to: customer information, personnel records, maps, diagrams, topologies and collectively "data" in paper, electronic or film form and regardless of how it is stored or transmitted.

3.1 FERC Critical Energy Infrastructure Information (CEII)

CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

- *Relates details about the production, generation, transmission, or distribution of energy.*
- *Could be useful to a person planning an attack on critical infrastructure.*
- *Is exempt from mandatory disclosure under the Freedom of Information Act; and*

**AES US SBU
Policies**

Document Control No.: **IS-010**
Last Revised Date: **6-4-2015**
Page **2**

US SBU INFORMATION CLASSIFICATION POLICY

- Gives strategic information beyond the location of the critical infrastructure.
- US SBU Business Information in which the business owner has defined its value, criticality, sensitivity or legal implications in which the business owner included in this policy to differentiate between various levels of sensitivity and value.

The US SBU Information Classification Policy does not restrict or supersede other information classification standards, requirements, policies or procedures that are more stringent and/or regulated as part of the following NERC CIP standards:

- NERC CIP-003-3 R4: Information Protection
- NERC CIP-011-5: Information Protection Effective Dates
- NERC CIP-014-1: Security for Critical Substations

4.0 DEFINITIONS

The terms and definitions listed below are meaningful for this policy:

4.1 Anonymized / Anonymization:

The process of rendering information into an irrevocable form which does not identify any individual and can no longer be linked to an individual.

4.2 Backup:

The process of making copies of files and other information electronically or physically stored to ensure they will be preserved in case of equipment failure, loss or theft etc.

4.3 Breach of Confidentiality:

The situation where confidential or restricted information has been put at risk of unauthorized disclosure as a result of the loss or theft of the information or, the loss or theft of a computer device containing a copy of the information or through the accidental or deliberate release of the information.

4.4 Electronic Media:

Any information that has been created and is stored in an electronic format, including but not limited to software, electronic documents, photographs, video and audio recordings.

4.5 Encryption / Encrypt:

The process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorized persons.

**AES US SBU
Policies**

Document Control No.: **IS-010**
Last Revised Date: **6-4-2015**
Page **3**

US SBU INFORMATION CLASSIFICATION POLICY

4.6 Encryption Key:

A piece of information (i.e. a password, certificate, etc.) used to encrypt/decrypt information.

4.7 Information Technology (I.T.):

Includes all computer facilities and devices, networks and information communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and information that are owned or leased by AES US.

4.8 Media:

The systems that carry messages or data, i.e., the information "container." Format types include paper, microform, and electronic. Some examples are email, flash drives, hard drives, CDs, DVDs, floppy disks, servers, imaging systems, databases, data files, video, and voice recording systems.

4.9 Mobile Computing Device:

Any handheld computer device including but not limited to laptops, notebooks, tablet computers, iPads, smartphone devices (e.g. PDA, iPhone and Blackberry enabled devices, etc.).

4.10 Non-Disclosure (and Confidentiality) Agreement:

An agreement established between the affected parties governing the disclosure of Information.

4.11 Owner:

The individual(s) responsible for or knowledgeable about how the information is generated, created, acquired, transmitted, stored, deleted, or otherwise processed.

4.12 Personal Identifiable Information – PII (as defined by NIST):

Any information about an individual maintained including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

4.13 Personal Use:

The use of the Information Technology (IT) resources for any activity(s) which is not work-related.

4.14 Pulverize / Pulverized:

Destruction by grinding into very small pieces or powder.

**AES US SBU
Policies**

Document Control No.: **IS-010**
Last Revised Date: **6-4-2015**
Page 4

US SBU INFORMATION CLASSIFICATION POLICY

4.15 Removable Storage Device:

Any optical or magnetic storage device or media, including but not limited to: CD, DVD, magnetic tapes, USB flash drive (i.e. memory stick/pen/keys), external/portable hard drives.

4.16 System Owner:

The individual(s) responsible for the maintenance and support of the system where the data is generated, accessed, transmitted or stored.

4.17 Structured Data:

Data associated with a business application or system. Data that resides in fixed fields within a record or file; relational databases and spreadsheets are examples of structured data.

4.18 Unstructured Data:

Data not associated with a business application or system. Data that does not reside in fixed locations. Examples are any protected documents such as: word processing documents, excel spreadsheets, PDF files, e-mail messages, blogs and/or web pages.

4.19 User:

The individual(s), organization or entity that interacts with data for the purpose of performing an authorized task.

US SBU INFORMATION CLASSIFICATION POLICY

5.0 POLICY

The following policy for Information Classification affects all business activity across the US SBU.

5.1 Information Classification

All information (irrespective of its format) owned, created, received, stored and processed by the US SBU must be classified according to the sensitivity of its contents. Classification controls should take account of the organizational needs for sharing or restricting the information and the associated impacts and risks (e.g. consequences if information is handled inappropriately). All information owned, created, received, stored or processed by the US SBU must be classified into one of following categories:

- *Public/Unclassified*
- *Internal*
- *Confidential*
- *Restricted information*

5.2 Public/Unclassified Information

Public/Unclassified information is defined as information that is available to the general public and is intended for distribution potentially outside of the organization. There would be no impact to the US SBU, its personnel, clients or business partners if this type of information was mishandled or accidentally released. Some examples of public information include:

- *Company Brochures*
- *Staff Brochures*
- *News or media releases*
- *Pamphlets*
- *Advertisements*
- *Web content*
- *Job postings*

5.3 Internal Information

Internal information is defined as information that is only intended for internal distribution among US SBU personnel, contractors, sub-contractors, agency staff and authorized third parties (i.e. service providers etc.). In the majority of instances there would be no significant impact on AES US if this type of information was mishandled or accidentally released. Some examples of internal information include:

- *Internal telephone directory*
- *User manuals*
- *Organizational newsletters & magazines*

US SBU INFORMATION CLASSIFICATION POLICY

5.4 Confidential or Restricted Information

Confidential information is highly sensitive which is protected by legislation or regulations, legal contracts or internal policy. The unauthorized or accidental disclosure of this information could seriously and/or adversely impact the US SBU, its personnel, customers and business partners.

Restricted information is highly sensitive which is protected by legislation or regulations, legal contracts or internal policy. The unauthorized or accidental disclosure of this information could seriously and/or adversely impact the US SBU, its personnel, customers and business partners.

Some examples of confidential or restricted information include the following applicable examples:

- *HR/personal records*
- *Financial information / budgetary reports*
- *Service plans / service performance monitoring reports*
- *Draft reports*
- *Audit reports*
- *Purchasing information*
- *Vendor contracts / commercially sensitive information*
- *Information covered by non-disclosure / confidentiality agreements*
- *Passwords / cryptographic private keys*
- *Information collected as part of criminal investigations*
- *Unpublished financial reports*
- *Strategic corporate plans*
- *Information regulated by FERC/NERC requirements*
- *Information related to customer accounts (PII)*

Information regarded as Confidential or Restricted must be handled in accordance with the Information Classification Matrix, (Appendix A) and any release outside of the organization must be approved by the business owner(s) and with an executed US SBU Non-Disclosure Agreement (Appendix B) in place.

5.5 Protective Markings

Protective markings indicate to other people the information classification category, and level of protection needed in handling, transferring and storing the information. As the business owner decides which classification category applies to information, they must communicate this to others by displaying the classification category on the document or file; protectively marking the document or file to help others to understand the level of protection that shall apply when they handle, transfer or store that information. Show the protective marking (i.e. Public or Unclassified, Internal, Confidential, or Restricted) in a prominent place such as a watermark(s) headers, footers, or stamps; emails shall also contain a notice.

**AES US SBU
Policies**

Document Control No.: **IS-010**
Last Revised Date: **6-4-2015**
Page **7**

US SBU INFORMATION CLASSIFICATION POLICY

5.6 Disclosing Information

The US SBU will not give access, disclose, or transmit Confidential or Restricted Information to any person or entity that is not authorized to have access to, review, or otherwise see the Information classified as Confidential or Restricted. Special procedures are followed if Confidential or Restricted information is needed in the event of audits or investigations. See Procedures referenced in Appendix A for details.

5.7 Reporting Improper Disclosure or Loss

Internal users or owners must promptly notify their departmental manager, any member of the management team, the Infrastructure Security team and/or the US SBU legal department regarding any accidental or unauthorized disclosure or loss of Internal, Confidential, or Restricted Information created, received or maintained by the US SBU. This Policy in no way limits other US SBU policies and procedures from requiring more specific notification requirements as mandated by regulatory or legal requirements. Issues of Improper disclosure or loss of Internal, Confidential, or Restricted Information are to be treated as "need to know" and should not be discussed internally or externally without written approval of executive management or the US SBU legal department, or as required by law.

**AES US SBU
Policies**

Document Control No : **IS-010**
Last Revised Date: 6-4-2015
Page 8

US SBU INFORMATION CLASSIFICATION POLICY

5.8 Example Matrix

The example below is an example of Appendix A.

| | Public/Unclassified | Internal | Confidential | Restricted |
|------|---|---|---|---|
| | <p>Information that is available to the general public and intended for distribution outside the organization</p> <p>This information may be freely disseminated without potential Harm.</p> | <p>Information that is only intended for internal distribution among US SBU staff and authorized third parties (i.e. service providers, contractors and sub-contractors).</p> | <p>Confidential information is highly sensitive which is protected by legislation or regulations, legal contracts or internal policy.</p> | <p>Restricted information is highly sensitive which is protected by legislation or regulations, legal contracts or internal policy.</p> |
| | <ul style="list-style-type: none"> Company brochures; Staff Brochures; News or media releases; Pamphlets; Advertisements; Web content; Job postings. | <ul style="list-style-type: none"> Internal telephone directory; User manuals; Staff newsletters & magazines. | <ul style="list-style-type: none"> HR/personal records; Financial information / budgetary reports; Audit reports; Purchasing information; Vendor contracts / commercially sensitive information; Information covered by non-disclosure / confidentiality agreements; Passwords / cryptographic private keys; Information collected as part of criminal investigations; Strategic corporate plans; Information regulated by FERC/NERC requirements; Information related to customer accounts (PII). | <ul style="list-style-type: none"> HR/personal records; Financial information / budgetary reports; Audit reports; Purchasing information; Vendor contracts / commercially sensitive information; Information covered by non-disclosure / confidentiality agreements; Passwords / cryptographic private keys; Information collected as part of criminal investigations; Strategic corporate plans; Information regulated by FERC/NERC requirements; Information related to customer accounts (PII). |
| None | | <p>In the majority of instances the unauthorized disclosure would not significantly impact the organization.</p> | <p>The unauthorized or accidental disclosure of this information could seriously and/or adversely impact the US SBU, its staff, customers and business partners.</p> | <p>The unauthorized or accidental disclosure of this information could seriously and/or adversely impact the US SBU, its staff, customers and business partners.</p> |

US SBU Information Classification Matrix

**AES US SBU
Policies**

Document Control No.: **IS-010**
Last Revised Date: **6-4-2015**
Page **9**

US SBU INFORMATION CLASSIFICATION POLICY

5.9 Safeguarding and Handling of Information

The following safeguards and handling considerations shall be implemented as part of the information classification policy:

- *Information must be limited only to those with business need.*
- *Internal, Confidential, and Restricted information must be marked as such.*
- *Confidential and Restricted information shall be stored inside a secure perimeter or in another secured fashion (i.e. locked cabinet) when not actively in use.*
- *If the physical and electronic information is to leave a secured area, it shall be in the possession of authorized personnel at all times. Electronic data shall be encrypted.*
- *Information shall not be provided to third party personnel unless the third party personnel are authorized and a current Non-disclosure agreement is executed.*
- *Care must be taken when Confidential and Restricted information discussions take place in a public area where conversations can be overheard.*

5.10 Disposal and Asset Reuse

The disposal, reuse or reallocation of records shall adhere to following guidelines:

- *Physical records no longer required shall be disposed of in a manner that protects the confidentiality and sensitivity of the record. Confidential and Restricted physical documents shall be cross-cut shredded or otherwise destroyed to ensure that information is not reasonably recoverable.*
- *Data assets (i.e. hard drives, memory sticks, etc.) must be wiped or re-imaged prior to any redeployment.*
- *A Data asset that needs to be returned in "as-is" state to the manufacturer will be sent via bonded, secure messenger in a sealed case. The vendor will maintain a service document to reference the asset.*
- *Any asset containing sensitive information deemed for disposal will have all storage media destroyed using one of the following methods:*
 - *Degaussing for a minimum of 10 seconds per side.*
 - *Data wiped to meet DoD 5220.22-M Standards.*
 - *Crushing the drive using a hydraulic crusher.*

6.0 CONFLICTS

If there is a conflict between this Policy and another US SBU policy or procedure, the more restrictive policy or procedure shall be followed.

7.0 POLICY ENFORCEMENT

**AES US SBU
Policies**

Document Control No.: **IS-010**
Last Revised Date: 6-4-2015
Page 10

US SBU INFORMATION CLASSIFICATION POLICY

This policy will be enforced by local management. Failure to follow this policy may result in disciplinary action, up to and including termination of employment.

8.0 POLICY EXCEPTIONS

None.

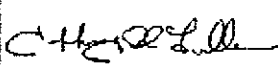
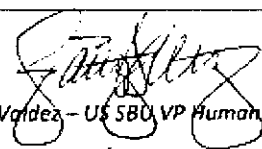
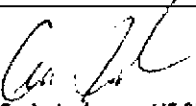
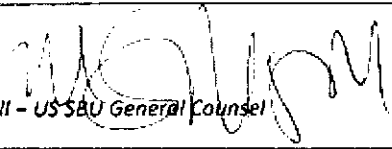
9.0 STANDARDS AND GUIDELINES

Reference the US SBU Cyber-security Plan, NERC CIP and all local, state, federal and regulatory requirements, standards, and guidelines referencing the protection of data as applicable.

10.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:

| | |
|--|-----------------|
|  Fuller, Jeffrey K Director, Cyber and Physical Security Jun 22 2015 4:15 PM Jeffrey Fuller – Director, US SBU Infrastructure Security | Date |
|  James Valdez – US SBU VP Human Resources | 7/6/15 Date |
|  Craig Jackson – US SBU CFO | 6/30/15 Date |
|  Mike Mizell – US SBU General Counsel | 7/6/15 Date |

**AES US SBU
Policies**

Document Control No.: **IS-010**
Last Revised Date: **6-4-2015**
Page **11**

US SBU INFORMATION CLASSIFICATION POLICY

11.0 Version Control History

| Date | Description of Changes | Author(s) |
|-------------------|---|-------------------------|
| February 19, 2015 | Initial Policy creation | Infrastructure Security |
| April 6, 2015 | Minor edits to punctuation and grammar. | Infrastructure Security |
| June 4, 2015 | Edits to place into US SBU template | Infrastructure Security |

**AES US SBU
Policies**

Document Control No. **IS-010**
Last Revised Date: **6-4-2015**
Page **12**

US SBU INFORMATION CLASSIFICATION POLICY

12.0 Appendix A: Information Classification and Handling Matrix

A procedural matrix has been developed to guide personnel in assigning a classification to information based on specific topics.

The Information Classification and Handling Procedural Matrix shall be used as a reference to the US SBU Information Classification Policy. A sample of the tables used to present the information is shown in diagram 1, below.

| Topic | Public/Unclassified | Internal | Confidential | Restricted |
|---------------------|----------------------------|---------------------|---------------------|---------------------|
| Sample Topic | <i>Sample text.</i> | <i>Sample text.</i> | <i>Sample text.</i> | <i>Sample text.</i> |

(Diagram 1)

See the 'Information Classification and Handling Procedural Matrix' for full details.

Security – Exhibit 3

Listing of Security Standards

- **US CERT** (United States Computer Emergency Readiness Team) Standards
- **ES-ISAC** (Electricity Sector Information Sharing & Analysis Center)
- **SANS** (System Administration, Networking, and Security Institute)
- **CVSS** (Common Vulnerability Scoring System)
- **DOE ES-C2M2** (Dept. of Energy Electricity Subsector Cyber-security Capability Maturity Model)
- **ISO/IEC 27000** (International Organization for Standardization & International Electrotechnical Commission)
- **NIST 800** (National Institute of Standards and Technology)
- **PCI DSS** (Payment Card Industry Data Security Standard)
- **FERC** (Federal Energy Regulatory Commission)
- **NERC** (North American Electric Reliability Corporation)
 - NERC CIP v3
 - NERC CIP v5
 - NERC CIP 014
- **US SBU (DP&L) Cyber-security Plan**
- **US SBU (DP&L) Physical Asset & Personnel Security Plan**
- **DHS CFATS** (Department of Homeland Security Chemical Facility Anti-Terrorism Standards)

Security – Exhibit 4

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> |
| | | Last Revision <u>11/12/2013</u> |

| <u>APPLICABILITY</u> | <u>TYPE</u> | <u>SENSITIVITY</u> |
|---|--|--------------------|
| Business Unit | Procedure | Business Private |
| <u>COMPLIANCE</u> | | |
| [Check all that apply] | | |
| <input type="checkbox"/> FERC Code of Conduct | <input type="checkbox"/> PUCO Code of Conduct | |
| <input type="checkbox"/> NERC Reliability Standards | <input type="checkbox"/> PUCO CAM | |
| <input checked="" type="checkbox"/> NERC Compliance | <input type="checkbox"/> PUCO Reliability Compliance | |
| <input checked="" type="checkbox"/> NERC Data Confidentiality | <input type="checkbox"/> Other [please specify]: | |
| <input type="checkbox"/> SOX | <input type="checkbox"/> None | |

1.0 Purpose

This Cyber Security Policy represents management's commitment and ability to secure its BES Cyber Assets. This Policy requires that critical systems maintain an effective level of cyber security and provides a framework for compliance with NERC standards CIP-004 through CIP-011.

2.0 Scope**1. Policy Statement**

This Policy applies to all Critical Systems used by the Company in its NERC Registered Functions: Transmission Owner, Generation Owner, Generation Operator, Load Serving Entity, Purchasing/Selling Entity and Distribution Provider.

Exceptions to this Policy may be made in whole or part during an emergency situation. An emergency situation is generally defined as a serious situation that happens unexpectedly, demands immediate action and that may poses an immediate risk to a life, health or property.

In the event of an emergency situation the Senior Manager and/or delegate must be notified as soon as possible and practical. The emergency situation must be documented within 30 calendar days and will be reviewed by the Senior Manager or delegate with the responsible supervisor(s), manager(s), director(s) or other authorized individuals.

3.0 Definitions

See Glossary and Definition document.

| | | |
|---|--|--|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>2</u> Last Revision <u>11/12/2013</u> |

4.0 Contents and Documents



Section: 1. Cyber Security – Personnel and Training

CIP Reference: CIP-004 R1, R2

Summary: Establish, maintain and document an annual cyber-security training program and a Cyber Security awareness program.

Policy: Provide and maintain a Cyber Security training program for personnel based on their role in the organization.

The required training associated to the roles will be based on the functions of that specific job within the CIP environment. The training subjects will include, but not be limited to:

- Physical Access Controls
- Visitor Management Program
- Cyber Security Policy
- Electronic Access Controls
- Handling of BES Cyber System Information and Storage
- Cyber Asset Access Control and Risks.
- Cyber Asset Acceptable Use
- Identification of Cyber Security Incidents
- Response to Cyber Security Incidents
- Recovery Plans for BES Cyber Assets
- Cyber Security Risks and Mitigation Measures

In addition to the role based training that personnel receives the Infrastructure Security team will develop and maintain a security awareness program that shall be made available to all personnel having authorized cyber or authorized unescorted physical access to Critical Systems. The program shall provide on-going reinforcement in sound security practices on at least a quarterly basis.

In an emergency situation, access may be granted to a Critical System before cyber-security training occurs. Training must occur as soon as possible after emergency access has been granted. Granting of emergency access for any of the defined PSPs shall be documented, approved by the Vice President of the business area where the PSP resides or the CIP Senior Manager or a delegate of the CIP Senior Manager before access is granted. All requests are reviewed by the Senior Manager.

In the event of an emergency situation the Senior Manager and/or delegate

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |

must be notified as soon as possible and practical. The emergency situation must be documented within 30 days and will be reviewed by the Senior Manager or delegate with the responsible supervisor(s), manager(s), director(s) or other authorized individuals.

Document(s): 7.1) CYBER PROC 004 Training, Awareness & Personal Risk Assessment

| | | |
|--|--|--|
| Original Issue Date <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision <u>11/12/2013</u> |

Section: 2. Personnel Risk Assessment

CIP Reference: CIP-004 R3
Corporate Policy—Personnel Risk Assessment

Summary: Establish, maintain and document a personnel risk assessment program

Policy: A personnel risk assessment program shall be created, maintained and documented for all personnel having access to BES Cyber Systems. The program shall be conducted in accordance with all existing federal, state and local laws and be administered by Human Resources. The risk assessment shall be conducted before access is granted to the Critical System and shall be updated at least every 7 years or for cause. The risk assessment shall include at a minimum identity verification and 7 year criminal check.

In an Emergency Situation access may be granted to a Critical System before the personnel risk assessment is complete. The risk assessment must occur as soon as possible after emergency access being granted. Granting of emergency access for any of the defined PSPs shall be documented, approved by the Vice President of the business area where the PSP resides or the CIP Senior Manager or a delegate of the CIP Senior Manager before access is granted. All requests are reviewed by the Senior Manager.

Document(s): 8.1) CYBER PROC 004 Training, Awareness & Personal Risk Assessment

| | | |
|---|--|--|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>2</u> Last Revision <u>11/12/2013</u> |

Section: 3. Authorized Access Review

CIP Reference: CIP-004 R4

Summary: Establish, maintain and document a program to verify unescorted physical and electronic access is required for an individual

Policy: Individuals that have unescorted physical or electronic access to a BES Cyber Asset will have their access reviewed on a quarterly basis to ensure that they have a continuing business need for the access. If access is no longer required it will be revoked.

In an Emergency Situation access may be maintained to a BES Cyber Asset after business need has been shown to have expired. A risk assessment must occur and the access must be documented and approved by the Senior Manager or the EMS Supervisor or the VP in charge of the area where the Cyber Asset is located. The Senior Manager will review all requests for emergency access.

Document(s): 8.2) CYBER PROC 004 Training, Awareness & Personal Risk Assessment

| | | |
|---|--|--|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>6</u> Last Revision <u>11/12/2013</u> |

Section: 4. Access Revocation

CIP Reference: CIP-004 R5

Summary: Establish, maintain and document a program to remove access to BES Cyber Assets

Policy: Individuals that have unescorted physical or electronic access to a BES Cyber Asset will have their access revoked within 24 hours of termination, retirement, or any transfer that would eliminate the business need to access specific BES Cyber Assets.

Shared accounts whose passwords are known by the individual whose access is being revoked will be changed within 30 calendar days from the date that the Infrastructure Security Team determines that the individual no longer requires access to the account.

In an Emergency Situation any shared accounts whose passwords are known by the terminated/transferred individual can be maintained past the 30 calendar days. In this case the reasons for the delay must be documented and approved by the Senior Manager. The shared password must be changed within 10 calendar days following the end of the emergency circumstances.

Document(s): 8.3) CYBER PROC 004 Training, Awareness & Personal Risk Assessment

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision: <u>11/12/2013</u> |

Section: 5. Electronic Security Perimeter (ESP)

CIP Reference: CIP-005 R1

Summary: All applicable Cyber Assets connected via a routable protocol must reside within an Electronic Security Perimeter

Policy: An Electronic Security Perimeter shall be defined around each network containing one or more Cyber Assets. If a Cyber Asset is accessible only by a dial-up telephone line (such as in a substation), then the Electronic Security Perimeter shall be defined around the dial-up device. Each Electronic Security Perimeter shall be identified and documented.

All electronic access points for systems outside the Electronic Security Perimeter to communicate with systems inside the Electronic Security Perimeter shall be identified and documented.

Access points will deny all access by default. Only approved communication ports will be allowed. Documentation of the approved ports will include the business processes that require the communication port to be opened and will show only permitted access is allowed.

Electronic access points for high impact BES cyber-systems or medium impact BES cyber-systems at control centers will have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

Each Computer System or Network Device within an Electronic Security Perimeter which communicates with a routable protocol shall be identified as a Critical Asset or as a component of a Critical System. Each Electronic Security Perimeter, with its network access control and monitoring systems, shall be considered a separate Critical System.

All Critical Systems within an ESP shall be subject to the collective Cyber Security Policies and shall meet the requirements of the highest impact BES Cyber System that is in the zone.

Documentation related to each Electronic Security Perimeter shall be updated as soon as practical after an Electronic Security Perimeter is modified, but in no case more than 30 calendar days after such modification. Documentation for all Electronic Security Perimeters shall be reviewed at least annually and records of such reviews kept.

Document(s): 9.1) CYBER PROC 005 Electronic Security Perimeter Procedure

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |

Section: 6. Interactive Remote Access Management

CIP Reference: CIP-005 R2

Summary: Interactive remote access to selected BES Cyber Systems to perform troubleshooting and system monitoring support is allowed.

Policy: Remote access into BES Cyber Systems will be initiated across intermediate systems located on the corporate network, DMZ and within the ESP; there will be no remote access session that accesses a BES Cyber Asset directly. Each intermediate system will be used to authenticate, monitor and log remote access sessions.

Encrypted tunnels will be created between all intermediate systems to prevent interception of sensitive data during a remote access session.

Multi factor authentication will be used when connecting to the intermediate systems on the corporate network and within the DMZ to ensure that only authorized personnel will have remote access to BES Cyber Systems.

Authentication, Authorization and Accounting (AAA) services will be used to restrict and monitor remote access through the intermediate system located in the DMZ between the corporate and TransOps network.

Document(s): 10.1 CYBER PROC 005 Electronic Security Perimeter Procedure

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |

Section: 7. Physical Security of BES Cyber Systems

CIP Reference: CIP-006 R1, R2, R3

Summary: Each Electronic Security Perimeter shall be protected by a Physical Security Perimeter as defined by a Physical Security Plan. Physical security systems shall be tested and maintained at least annually.

Policy: To assure good physical security, one or more Physical Security Plans shall be developed, implemented and monitored.

Each Physical Security Plan shall define and shall apply to one or more Physical Security Perimeters. All Cyber Assets residing within an Electronic Security Perimeter shall also reside within a Physical Security Perimeter. Each Physical Security Plan shall ensure the following:

1. Each Physical Security Perimeter where feasible shall consist of at least two physical access controls to restrict physical access to the Cyber Assets contained within.
2. Physical Access Control Systems (PACS) that make up the inner core of the security perimeter will follow the provisions defined by the Access Control and Monitoring and the Change Control and Configuration Management section of the Cyber Security Policy.
3. Each access point through a Physical Security Perimeter shall be identified, documented and controlled.
4. Entry procedures for each security perimeter will be defined and will be a part of the Security Training section of the Cyber Security Policy.
5. Each entry or attempted entry through an access point shall be logged. Logs will be kept for at least 90 calendar days.
6. When detected, unauthorized access or attempted access shall be investigated and remedial action taken and documented.
7. Authorized access shall be clearly defined and shall include, where appropriate, provisions for visitor access, vendor access and emergency situations. Unauthorized access shall be prohibited.
8. Unescorted access to a Physical Security Perimeter shall only be granted in accordance with established procedures regarding the Personnel Risk Assessment and Training and appropriate Authorization(s) as specified in Cyber Security Policy.
9. Individuals not authorized for unescorted access shall be considered as 'Visitors' and shall be escorted at all times. Each Physical Security Plan shall

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | <p align="center">DPL Business Practice</p> <p align="center">Critical Infrastructure Protection</p> <p align="center">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |

define the meaning of "escorted access" clearly and unambiguously.

10. A visitor management procedure will be defined for each Physical Security Plan. The visitor management procedure will describe the logging mechanisms in use. Visitor logs will be kept for a minimum of 90 calendar days.
11. Each Physical Security Plan shall be updated within 30 calendar days of any redesign or reconfiguration of the plan or any components used to implement the plan.
12. Each Physical Security Plan shall be reviewed at a frequency specified in the Plan. The frequency of review shall not be more than annually. Each review of each Physical Security Plan shall be documented and shall be approved by a Senior Manager or delegate.
13. All devices used in the implementation of a Physical Security Plan shall be tested on a scheduled basis. The testing cycle may not exceed 12 calendar months.
14. Records of outages regarding access control systems, logging systems or monitoring systems shall be kept. These records shall be retained for a rolling three year period.
15. If any PACS device becomes inoperable and repair is not possible within 5 minutes of its loss, mitigation measures shall be developed, implemented and documented.

In an Emergency Situation access to a Physical Security Perimeter may be granted to first responders or other personnel required to meet the needs of the emergency. The situation that caused emergency access to be granted will be documented within 10 calendar days of the conclusion of the emergency and the document will be reviewed and approved by the CIP Senior Manager or a delegate.

Documents(s): 13.1) CYBER PROC 006 Physical Security of Cyber Assets Procedure

□

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |



Section: 8. Ports and Services

CIP Reference: CIP-007 R1

Summary: Only the ports and service that are required for operations will be enabled, all other ports will be disabled when technically feasible.

Policy: On each Cyber Asset as feasible, each service that opens one or more Network Ports must be documented with the service name, protocol and port number(s) it opens. The purpose, business need and measures taken to protect each service must also be indicated.

Any unused or unneeded services and the associated ports must be disabled if technically feasible. Those services that cannot be disabled must be documented and the exposure thus created must be mitigated. The documentation must include the reason the service cannot be disabled and the steps taken to mitigate the exposure.

On each network protection device which controls access to Cyber Assets, each open port and its associated service must be documented. The network protection device's rule set must be reconciled at least annually with the Critical System documentation.

Physical input/output devices will be protected by one or more of the following methods; through system configuration, by the use of a third party application, group policy settings on the domain, a physical obstruction of the port, and/or through the use of signage.

In an emergency situation ports may be opened only with the consent of the Senior Manager or their delegate. The situation that caused emergency port access to be granted will be documented within 10 calendar days of the conclusion of the emergency and the document will be reviewed and approved by the Senior Manager or a delegate.

Document(s): 10.1 CYBER PROC 007 Systems Security Management

□

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>2</u> Last Revision: <u>11/12/2013</u> |

Section: 9. Security Patch Management

CIP Reference: CIP-007 R2

Summary: Security patches on all Critical Systems shall be kept up to date.

Policy: For each Cyber Asset, an inventory of all software and firmware shall be kept. Each item in the inventory shall be monitored for the availability of security patches.

At least once every 35 calendar days security patches shall be evaluated for applicability to installed devices or software.

Any patch that is deemed applicable shall be tested and an implementation plan developed within 35 calendar days of the evaluation completion.

If testing of a patch exposes an issue that adversely affects any Cyber Asset, that patch need not be installed. Instead, a dated mitigation strategy shall be developed or an existing mitigation plan will be revised.

Each security patch identified, whether applicable or not, shall be tracked and documented. The tracking documentation shall record, at a minimum, the affected system(s), the identifying name or number of the patch, the evaluation of applicability, the results of testing, and the final disposition of the patch, including any mitigation strategy. The tracking documentation shall record the dates of all significant events in this process.

Document(s): 10.1 CYBER PROC 007 Systems Security Management

| | | |
|---|--|--|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision <u>11/12/2013</u> |



Section: 10. Malicious Software Prevention

CIP Reference: CIP-007 R3

Summary: Malicious software prevention measures shall be taken for each system.

Policy: Each Cyber System within an Electronic Security Perimeter shall implement malicious software prevention measures. Where technically feasible, these measures shall include at least host-based anti-virus software.

Any virus updates, including signatures or patterns, will be tested in an environment that is as similar as technically feasible to the production environment before being deployed to production computer systems.

If testing reveals that any of these measures poses an unjustified risk to the reliability of the subject Computer System, that measure shall not be installed. Instead a mitigation strategy shall be developed and implemented.

If a Critical System implements malicious software prevention measures, a procedure for obtaining, testing and implementing updated Signature Files shall be documented and implemented.

If a specific Cyber Asset has no updatable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

When malicious code is detected on a Cyber Asset, the threat posed by that code will be mitigated by removing or quarantining the malicious code, or by physically removing the Cyber Asset from the network when feasible.

Document(s): 10.1 CYBER PROC 007 Systems Security Management

□

| | | |
|--|---|---|
| Original Issue Date <u>11/12/2013</u> | <p align="center">DPL Business Practice</p> <p align="center">Critical Infrastructure Protection</p> <p align="center">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number 2 Last Revision: <u>11/12/2013</u> |



Section: 11. Monitoring and Logging

CIP Reference: CIP-007 R4

Summary: Monitoring, Logging and Alerts of cyber related system events will be established

Policy: All Cyber Assets within the defined ESP(s) will be monitored using identified audit policy settings, managed where applicable through Group Policy.

Automated tools or organizational process controls will be utilized, where technically feasible, to monitor system events that are related to cyber security.

System logs will be captured. Software will be in place to monitor and report events on the BES Secure Network. Where technically feasible, the security monitoring process(es) will detect and alert for attempts at or actual unauthorized access.

Monitoring will be based upon addition, modification or removal of the following:

- Windows File system
- Windows Registry
- Active Directory Schema
- Linux File system
- EMS Cluster Windows and Oracle Directories
- Network Devices
- SCADA and RTUCS directories
- Device Configuration Settings
- Firmware Versions

Where technically feasible, Infrastructure Security Personnel will receive real-time alerts 24X7 365 days a year.

Collected logs will be retained for at least 90 consecutive calendar days.

For High Impact BES Cyber Systems and their associated EACMS and PCA, a summarization or sampling of the collected logs will be reviewed at least once each 15 calendar days to identify any undetected Cyber Security Incidents.

Including, but not limited to:

- Unsuccessful login attempts;
- Failed access attempts and failed login attempts; and
- Malicious code

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision: <u>11/12/2013</u> |

Document(s): 10.1 CYBER PROC 007 Systems Security Management

□

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | <p align="center">DPL Business Practice</p> <p align="center">Critical Infrastructure Protection</p> <p align="center">Cyber Security Policy</p> | Original Issue Date <u>11/12/2013</u> |
| | | Revision Number <u>9</u> Last Revision <u>11/12/2013</u> |



Section: 12. System Access Controls

CIP Reference: CIP-007 R5

Summary: System Access Control

Policy: Where technically feasible, access to protected systems will require authentication.

All generic or default accounts residing on protected assets will be identified and listed. Where technically feasible, generic or default accounts will be renamed, disabled or removed.

When technically feasible, all default passwords on protected systems will be changed. If the password cannot be changed, a mitigation process will be documented to protect the cyber asset.

All shared accounts used on protected assets will be listed and those people that have access to the shared accounts will be identified and approved on a quarterly basis.

For password only authentication the password will consist of, at a minimum, the following parameters:

- The password length will be at least 8 characters, or the maximum length supported by the Cyber Asset; and
- The password complexity will include the lesser of;
 - three or more character types (uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or,
 - the maximum complexity supported by the Cyber Asset.

When technically feasible, passwords used for interactive user access will be changed at least once every 15 calendar months. This process will be enforced technically or procedurally.

When technically feasible, accounts will be locked out after 3 authentication attempts

- Alerts will be generated after a threshold of authentication attempts is met.

Document(s): 10.1 CYBER PROC 007 Systems Security Management

Section: 13. Incident Response

□

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>0</u> Last Revision <u>11/12/2013</u> |

CIP Reference: CIP-008 R1, R2, R3

Summary: A Cyber Security Incident Response Plan shall be developed, documented, tested, and as necessary, executed.

Policy: A Cyber Security Incident Response Plan shall be developed for each Electronic Security Perimeter. Each Plan shall include, at minimum:

- The list of Electronic Security Perimeters for which the Plan is valid.
- A procedure for collecting and retaining security events from each Critical System within the Electronic Security Perimeter; these event logs shall be retained for at least 90 calendar days, or for at least three years if they are related to a reportable Cyber Security Incident.
- A mechanism for analyzing the security event logs to identify an event or series of events that comprises a Cyber Security Incident.
- A mechanism for classifying Cyber Security Incidents as reportable or non-reportable.
- An identified and trained Incident Response Team, including roles and responsibilities of each team member.
- The incident handling stance for each system covered by the plan (e.g., "observe and report", "contain and control").
- Incident handling procedures, including special considerations for certain systems.
- Communication plans.
- A procedure for communicating a reportable Cyber Security Incident to the ES-ISAC and other appropriate authorities.
- A process to evaluate each Cyber Security Incident (whether reportable, non-reportable or test) after the fact, including a "lessons learned" session for the entire Team.
- A process to implement any "lessons learned".
- A process to notify each person or group with a defined role in the Cyber Security Response Plan of any updates based on any documented "lessons learned".
- A process to update the Cyber Security Incident Plan(s) and notify each person or group with a defined role of any personnel or technical changes that would impact the ability to execute the plan.

Each Response Plan shall be tested at least once every 15 calendar months. Response to an actual Cyber Security Incident may be considered as a test of the relevant Response Plan.

For each reportable Cyber Security Incident, documentation of the incident and any forensic evidence obtained shall be kept for at least three years. This documentation and evidence shall be governed by the Information Protection

| | | |
|---|---|--|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>2</u> Last Revision <u>11/12/2013</u> |

Policy.

Document(s) 18.1) CYBER PROC 008 Incident Reporting and Response Planning Procedure

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |



Section: 14. Recovery Plans for BES Cyber Systems

CIP Reference: CIP-009 R1, R2, R3

Summary: A business continuity/disaster recovery plan shall be created, tested and maintained

Policy: For each Electronic Security Perimeter (ESP), a Recovery Plan shall be created. Each recovery plan shall contain, at minimum:

- The list of ESP(s) covered by the Recovery Plan.
- Events or conditions that will activate the Recovery Plan.
- Define roles and responsibilities of each responder.
- Processes and procedures for the backup, storage and recovery of information necessary to successfully restore operation of the affected Cyber Assets.
- Processes and procedures to show that backup processes completed successfully and any backup errors were addressed.
- Provision for a "lessons learned" session for each activation of the Recovery Plan, either during an actual event or test.
- Location of any required Backup Media.
- Processes to preserve data on a Cyber Asset when technically feasible for determining the cause of a cyber-security incident that triggered the activation of the recovery plan.

Each Recovery Plan shall be exercised at least once every 15 calendar months. An actual recovery of a BES Cyber Asset can be used as a substitute for this test.

Each recovery, either an actual or an exercise, shall include a "lessons learned" session after the exercise.

Each Recovery Plan that applies to a High Impact BES Cyber System shall have an operational exercise of the recovery plan performed at least once every 36 calendar months in an environment that is representative of the production environment.

After each "lessons learned" session, the appropriate Recovery Plan(s) shall be updated as needed. Changes to a Recovery Plan shall be made and communicated to the appropriate parties within 90 calendar days of the exercise or activation of the Recovery Plan.

The Plan(s) will be updated and people or groups with defined roles in the recovery plan notified within 60 calendar days of any change to the roles or responsibilities, responders, or technology that would impact the ability to

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>6</u> Last Revision: <u>11/12/2013</u> |

execute the recovery plan.

Backup Media containing information essential to recovery of a Cyber Asset shall be tested after any significant change to the backup or recovery procedures, hardware or software.

Document(s) 19.1) CYBER PROC 009 Recovery Plans for BES Cyber Systems

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |

Section: 15. Configuration Change Management and Vulnerability Assessments

CIP Reference: CIP-010 R1

Summary: Configuration Change Management

Policy: A baseline configuration will be created for all BES Cyber Assets, individually or by group, that will include at a minimum the following items:

- The Operating System(s) including version, or firmware where no independent operating system exists.
- Any commercially available or open-source application software, including version, intentionally installed.
- Any custom software installed.
- Any logical network accessible ports.
- Any security patches applied.

All hardware, software and configuration changes to shall be documented, approved and tested before being placed in production. All such changes shall be approved by the Senior Manager or designated alternate prior to being tested, and again prior to being placed in production.

Testing of changes shall be performed in a manner that minimizes adverse effects on the production system. Testing shall determine the impact of the change on the functionality and security of the production system.

Provision for Emergency Situations may be incorporated into the change control process. Exercise of any emergency provision shall be documented after the fact. In the event of an emergency situation the Senior Manager and/or delegate must be notified as soon as possible and practical. The emergency situation must be documented within 30 days and will be reviewed by the Senior Manager or delegate with the responsible supervisor(s), manager(s), director(s) or other authorized individuals.

A tracking and reporting system shall be established to document the status of approved and in-process changes and completed changes. The tracking system shall be used to assure approved changes are implemented as planned.

The tracking system will also incorporate an approval process that will be used to verify that all process owners are aware of the change to the Cyber Asset. Before any changes are made to a Cyber Asset, with the exception of Emergency Situations whose process is described above, all appropriate signatures will be added to the change management document.

As part of an approved change, the associated system and user documentation shall be updated as appropriate.

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>0</u> |
| | | Last Revision <u>11/12/2013</u> |

Development of software changes shall be on a system separate from the production environment.

Any changes to the existing baseline configuration the baseline configuration will be updated within 30 calendar days of completing the change.

Document(s) 19.1) CYBER PROC 010 – Configuration Change Management and Vulnerability Assessments.

| | | |
|--|---|--|
| Original Issue Date <u>11/12/2013</u> | <p align="center">DPL Business Practice</p> <p align="center">Critical Infrastructure Protection</p> <p align="center">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision <u>11/12/2013</u> |

Section: 16. Configuration Monitoring

CIP Reference: CIP-010 R2

Summary: Configuration Monitoring

Policy: All High Impact BES Cyber Systems and their associated EACMS and PCA's will be monitored for changes to the baseline configuration at least once every 35 calendar days and will include changes to:

- The Operating System(s) including version, or firmware where no independent operating system exists.
- Any commercially available or open-source application software, including version, intentionally installed.
- Any custom software installed.
- Any logical network accessible ports.
- Any security patches applied.

Any unauthorized changes will be documented and investigated.

Document(s) 19.1) CYBER PROC 010 – Configuration Change Management and Vulnerability Assessments.

| | | |
|---|--|--|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>9</u> Last Revision: <u>11/12/2013</u> |



Section: 17. Cyber Vulnerability Assessment

CIP Reference: CIP-010 R3

Summary: Network and Host Vulnerability Assessments shall be performed at least annually.

Policy: For each Electronic Security Perimeter (ESP), a Cyber Vulnerability Assessment Procedure shall be developed and implemented. These procedures shall discover and document all network access points to each ESP. These access points shall include, but not be limited to, all network connections, modem dedicated circuits, dial-up circuits, wireless connections and firewall rule sets.

For each Critical System within an ESP, a Critical System Vulnerability Assessment Procedure shall be developed and implemented. These procedures shall discover and document all open Network Ports.

For each access point (Network), or host (Computer System), each procedure shall:

- Identify the process used to perform the vulnerability assessment
- Ensure that only ports and services required for operations are enabled
- Review the controls for:
 - Default accounts
 - Shared administrative accounts
 - Password strength
 - Network management community strings
 - Any other potentially weak authentication mechanism
- Document the results of the assessment
- Develop, document and implement a plan to remediate or mitigate vulnerabilities identified by the assessment
- Track the status of the remediation or mitigation plan

Where prudent, a live vulnerability assessment shall be used.

Prior to each Vulnerability Assessment, the Senior Manager shall approve the procedure and scheduling for such assessment.

A summary of each Vulnerability Assessment shall be provided to the Senior Manager or delegate.

A paper or active vulnerability assessment will take place at least once every 15 calendar months for each Cyber System.

□

| | | |
|--|--|---|
| Original Issue Date <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision: <u>11/12/2013</u> |

For High Impact BES Cyber Systems and where technically feasible, an active vulnerability assessment will take place at least once every 36 calendar months.

For each of the assessments above, the results of the assessments will be documented and a plan will be documented to remediate or mitigate any vulnerability discovered during the paper or active assessments.

Prior to adding a new High Impact Cyber Asset to the production environment an active vulnerability assessment will be performed on the asset except in the case of CIP Exceptional Circumstances and like replacements of the same type of Cyber Assets with a baseline configuration that models an existing baseline configuration of the previous or other existing High Impact Cyber Asset.

Document(s): 12.1) CYBER PROC 010 – Configuration Change Management and Vulnerability Assessments.

| | | |
|---|--|--|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision <u>11/12/2013</u> |

Section: 18. Information Protection

CIP Reference: CIP-011 R1

Summary: Information associated with Critical Systems shall be identified, documented and protected.

Policy: An Information Protection Program shall be developed, documented and implemented to protect information associated with Cyber Assets.

The Information Protection Program shall identify and document information associated with Critical Systems including, but not limited to, the following:

- CIP Compliance Documents
- Operational Procedures
- Network Diagrams
- Computing Center Floor Plans
- Equipment Layouts
- Security Configurations
- Network Address Information

Information shall be identified regardless of mediatype or location.

An Information Classification System appropriate to the needs of cyber and physical security shall be developed and documented. All information identified as being associated with a Cyber Asset shall be classified based on the sensitivity of the information. Information shall be stored and handled in accordance with its classification.

A document management process shall be implemented for access control, retention and version management of appropriate documents relating to Critical Systems.

The effectiveness of the Information Protection Program and adherence to this Policy shall be assessed at least annually. This assessment shall be documented. A remediation plan shall be developed and executed to address any deficiencies identified by the assessment.

Document(s) 19.1) CYBER PROC 011 – Information Protection

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |



Section: 19. BES Cyber Asset Reuse and Disposal

CIP Reference: CIP-011 R2

Summary: BES Cyber Asset Reuse and Disposal

Policy: Each Critical System shall be subject to an information removal protocol appropriate to the system or device. Where feasible, such protocol may use portions of US DoD 5220.22 or equivalent process.

Any BES Cyber Asset that needs to be returned 'as-is' to the vendor for maintenance or troubleshooting will be sent via a secure messenger in a sealed and locked case. The vendor will be required to maintain a "Chain of Custody" document up to the point that any custom settings are destroyed. If the custom settings are unable to be destroyed, the memory in the device will be physically destroyed.

The "Chain of Custody" document will be kept as evidence for a minimum of 3 years.

Where technically feasible, Cyber Assets that are to be reused within an ESP will be returned to factory settings, or have their OS/Firmware reinstalled before they are configured for their new role.

If the system or device is to be Disposed of outside the Electronic Security Perimeter, the information removal protocol shall be used to remove all significant information from the system or device. The destruction of the asset will be documented and signed by the destructor.

Document(s) 19.1) CYBER PROC 011 – Information Protection

□

| | | |
|---|--|--|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision: <u>11/12/2013</u> |

A. GLOSSARY

| Term | Definition Source | Definition |
|------------------|-------------------|---|
| Annual | DPL Local | As defined by Merriam-Webster dictionary, annual is occurring or happening every year or once a year. Calendar year begins on January 1 and ends December 31. |
| Backup Media | DPL Local | Tapes, disks, or other removable media used to retain information that can be used to recover a Computer System in the event of the failure or destruction of that System. |
| BES Cyber Asset | NERC Glossary | A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.) |
| BES Cyber System | NERC Glossary | One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity. |

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | <p style="text-align: center;">DPL Business Practice</p> <p style="text-align: center;">Critical Infrastructure Protection</p> <p style="text-align: center;">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> Last Revision <u>11/12/2013</u> |

| Term | Definition Source | Definition |
|------------------------------|-------------------|--|
| BES Cyber System Information | NERC Glossary | Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System. |
| Bulk Electric System | NERC Glossary | As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition. |
| Business Owner | DPL Local | The management person responsible for the operation(s) supported by Critical Systems |
| CIP Exceptional Circumstance | NERC Glossary | A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability. |
| CIP Senior Manager | NERC Glossary | A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011. |

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> Revision Number: <u>0</u> Last Revision <u>11/12/2013</u> |
|---|---|---|

| Term | Definition Source | Definition |
|---|-------------------|--|
| Commercial Operations (CommOps) Network | DPL Local | The name given in reference to the EMS and supporting applications residing within the Electronic Security Perimeter enclave at MacGregor Park and the Backup Control Center. |
| Computer System | DPL Local | A set of hardware containing a general purpose or embedded computer with the ability to communicate via network, serial line or other method with another Computer System. |
| Control Center | NERC Glossary | One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. |
| Cyber Security Incident | NERC Glossary | A malicious act or suspicious event that: <ul style="list-style-type: none"> Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. |
| Electronic Access Control or Monitoring Systems | NERC Glossary | Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems. |
| Electronic Access Control or Monitoring Systems (EACMS) | NERC Glossary | Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems. |
| Electronic Access Point | NERC Glossary | A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter. |
| Electronic Security Perimeter (ESP) | NERC Glossary | The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. |
| Emergency Situation | DPL Local | A situation requiring immediate action to prevent harm to a Critical System or to the Bulk Electric System. |

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> Revision Number: <u>0</u> Last Revision <u>11/12/2013</u> |
|---|---|---|

| Term | Definition Source | Definition |
|--------------------------------|-------------------|--|
| (EMS) Energy Management System | DPL Local | Energy Management Systems (EMS) – A computer control system used by electric utility dispatchers to monitor the real time performance of the various elements of an electric system and to control Generation and transmission facilities. |
| EMS Supervisor | DPL Local | The person responsible for a Computer System, Network Device or Physical Security Perimeter. This responsibility extends to acquisition, change management and retirement of the System or Device |
| ESS Senior Manager | DPL Local | Individual delegated by the <i>Senior Manager</i> , to lead and manage the company's implementation of, adherence to, and execution of NERC Standards CIP-002 through CIP-009. |
| External Routable Connectivity | NERC Glossary | The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection. |
| Facility | NERC Glossary | A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.) |
| High Impact BES Cyber Systems | Standards | Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes. |
| Interactive Remote Access | NERC Glossary | User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications. |

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | <p align="center">DPL Business Practice</p> <p align="center">Critical Infrastructure Protection</p> <p align="center">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number <u>2</u> |
| | | Last Revision <u>11/12/2013</u> |

| Term | Definition Source | Definition |
|--|-------------------|---|
| Intermediate System | NERC Glossary | A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter. |
| Kiosk Account | DPL Local | A computer login account with limited functionality that is automatically activated upon system startup. |
| Medium Impact BES Cyber Systems | Standard | Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes. |
| Medium Impact BES Cyber Systems without External Routable Connectivity | Standard | Only applies to medium impact BES Cyber Systems without External Routable Connectivity. |
| Medium Impact BES Cyber Systems with External Routable Connectivity | | Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity. |
| Network Device | DPL Local | Router, firewall, switch or other device used to move data from one Computer System to another Computer System. |
| Network Port | DPL Local | In the TCP and UDP protocols used in computer networking, a port is a special number present in the header of a data packet. Ports are typically used to map data to a particular process or service running on a computer. |
| Physical Access Control Systems (PACS) | NERC Glossary | Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. |
| Physical Security Perimeter (PSP) | NERC Glossary | The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled. |
| Privileged Account | DPL Local | A login account on a Computer System or Network Device that permits administration of that System or Device. |

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | <p align="center">DPL Business Practice</p> <p align="center">Critical Infrastructure Protection</p> <p align="center">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>5</u> Last Revision: <u>11/12/2013</u> |

| Term | Definition Source | Definition |
|------------------------------------|-------------------|---|
| Protected Cyber Assets | NERC Glossary | One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. |
| Redeploy | DPL Local | The removal of a Computer System or Network Device from regular service inside an Electronic Security Perimeter, when its hardware is then used for another purpose. |
| Reportable Cyber Security Incident | NERC Glossary | A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. |
| Security Certification | DPL Local | A certification granted by a recognized security training or testing institution such as SANS or (ISC)². |
| Secure Area | DPL Local | Physical area surrounding cyber assets secured by physical and electronic security measures. |
| Senior Manager | DPL Local | The DPL executive designated by the CEO with overall responsibility and authority for leading and managing the company's implementation of, adherence to, and execution of NERC Standards CIP-002 through CIP-011. |
| Shared Operator Account | DPL Local | A computer login account with limited functionality that is shared among a group of operators for that system. |
| Signature Files | NERC Glossary | Those files containing signatures of computer viruses or other malware that are used to detect and prevent infection by said malware. |

| | | |
|---|---|--|
| Original Issue Date: <u>11/12/2013</u> | <p align="center">DPL Business Practice</p> <p align="center">Critical Infrastructure Protection</p> <p align="center">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision <u>11/12/2013</u> |

| Term | Definition Source | Definition |
|--|-------------------|---|
| Special Protection System (Remedial Action Scheme) | NERC Glossary | An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and Mvar), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include (a) under frequency or under voltage load shedding or (b) fault conditions that must be isolated or (c) out-of-step relaying (not designed as an integral part of an SPS). Also called Remedial Action Scheme. |
| TransOps Network | DPL Local | The name given in reference to the EMS and supporting applications residing within the Electronic Security Perimeter enclave at the Dayton Service Building and Backup Control Center. |

| | | |
|---|---|---|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> Revision Number: <u>2</u> Last Revision <u>11/12/2013</u> |
|---|---|---|



B. NERC CIP Standard Cross Reference

Standard Requirement

Policy Section(s)

CIP-004-5 Cyber Security – Personnel and Training

| | |
|-------------------------------|--|
| R1. Personnel and Training | 1) Cyber Security – Personnel and Training |
| R2. Personnel and Training | 1) Cyber Security – Personnel and Training |
| R3. Personnel Risk Assessment | 2) Cyber Security – Personnel and Training |
| R4. Authorized Access Review | 3) Cyber Security – Personnel and Training |
| R5. Access Revocation | 4) Cyber Security – Personnel and Training |

CIP-005-5 Electronic Security Perimeter

| | |
|--|---|
| R1. Electronic Security Perimeter | 5) Electronic Security Perimeter |
| R2. Interactive Remote Access Management | 6) Interactive Remote Access Management |

CIP-006-5 Physical Security of BES Cyber Systems

| | |
|--|---|
| R1. Physical Security Plan | 7) Physical Security of BES Cyber Systems |
| R2. Visitor Control Program | 7) Physical Security of BES Cyber Systems |
| R3. Physical Access Control System Maintenance and Testing Program | 7) Physical Security of BES Cyber Systems |

CIP-007-5 Systems Security Management

| | |
|-----------------------------------|-----------------------------------|
| R1. Ports and Services | 8) Ports and Services |
| R2. Security Patch Management | 9) Security Patch Management |
| R3. Malicious Software Prevention | 10) Malicious Software Prevention |
| R4. Monitoring and Logging | 11) Monitoring and Logging |
| R5. System Access Control | 12) System Access Controls |

CIP-008-5 Incident Response

| | |
|--|-----------------------|
| R1. Cyber Security Incident Response Plan | 13) Incident Response |
| R2. Cyber Security Incident Response Plan Implementation and Testing | 13) Incident Response |
| R3. Cyber Security Incident Response Plan Review, Update and Communication | 13) Incident Response |

Standard Requirement

Policy Section(s)

CIP-009-5 Recovery Plans for BES Cyber Systems

| | |
|--|--|
| R1. Recovery Plan | 14) Recovery Plans for BES Cyber Systems |
| R2. Recovery Plan Implementation and Testing | 14) Recovery Plans for BES Cyber Systems |
| R3. Recovery Plan Review, Update and Communication | 14) Recovery Plans for BES Cyber Systems |

CIP-010-1 Configuration Change Management and Vulnerability Assessments

| | |
|-------------------------------------|-------------------------------------|
| R1. Configuration Change Management | 15) Configuration Change Management |
| R2. Configuration Monitoring | 16) Configuration Monitoring |

| | | |
|---|--|---|
| Original Issue Date: <u>11/12/2013</u> | DPL Business Practice Critical Infrastructure Protection Cyber Security Policy | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>2</u> Last Revision: <u>11/12/2013</u> |

| Standard | Requirement | Policy Section(s) |
|----------|------------------------------------|------------------------------------|
| | R3. Cyber Vulnerability Assessment | 17) Cyber Vulnerability Assessment |

CIP-011-1 Information Protection

| | |
|---|---|
| R1. Information Protection | 18) Information Protection |
| R2. BES Cyber Assets Reuse and Disposal | 19) BES Cyber Assets Reuse and Disposal |

Review

This procedure will be reviewed annually from date of issuance.

| | | |
|---|---|--|
| Original Issue Date: <u>11/12/2013</u> | <p align="center">DPL Business Practice</p> <p align="center">Critical Infrastructure Protection</p> <p align="center">Cyber Security Policy</p> | Original Issue Date: <u>11/12/2013</u> |
| | | Revision Number: <u>0</u> Last Revision <u>11/12/2013</u> |

ACKNOWLEDGEMENTS AND APPROVALS

The following have reviewed and approved this policy:

Originated/Revised by:

Date:

Approved:

Date:



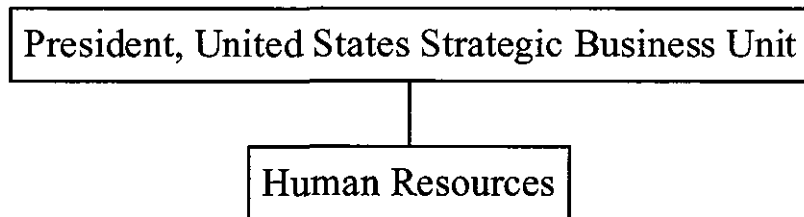
REVISION HISTORY

□

| Revision Number | Date Revised | Approved By | Revision Description |
|-----------------|--------------|-------------|----------------------|
| 0 | 12/26/2013 | | Original Document |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Human Resources

Human Resources has overall responsibility for employment related issues including recruiting, career development and benefits. The Human Resources function is described in detail in the following section.



Functional Area:
Human Resources

SFR Reference

- (B)(9)(h)(i) Salary and benefits**
- (B)(9)(h)(ii) Recruiting and selection**
- (B)(9)(h)(iii) Training and career development**
- (B)(9)(h)(iv) Performance evaluation and appraisal**
- (B)(9)(h)(v) Work force productivity**

Policy and Goal Setting:

Human Resources assists DP&L in achieving business goals by developing and maintaining the policies and programs aimed at attracting and retaining a talented workforce to safely and reliably deliver electric service to our customers.

As a member of the senior leadership team the Vice President of Human Resources participates annually in updating the long-term strategic business plan and developing short-term company goals. Human Resources leadership then reviews the Company's goals and sets annual departmental objectives to support those goals. The goals set by Human Resources leadership are reviewed by the US SBU senior leadership and are approved by the US SBU President.

Policies are generally formed at the leadership level and then brought before a Company policy committee for final review and approval. Human Resources leads the Company policy committee.

Strategic and Long-Range Planning:

Human Resources strategic planning efforts are aimed at attracting and retaining a talented workforce in order to further the Company's long-range strategy of delivering safe, reliable service to our customers. The people section of the long-term strategic business plan is developed by Human Resources leadership and focuses on objectives related to culture, total rewards, talent development, internal communications, and labor relations. Human Resources leadership annually updates the plan. It is then reviewed by US SBU senior leadership and approved by the US SBU President.

Organizational Structure and Responsibilities:

Human Resources consists of approximately 30 employees and is led by the Vice President of Human Resources. The goal of Human Resources is to assist the Company in achieving business objectives by attracting and retaining a talented workforce, maintaining positive employee and union relations while ensuring conformance to local, state, and federal regulations and requirements. Human Resources maintains responsibility for the following utility activities:

1. Total Rewards is responsible for the development and administration of fair and competitive compensation and employee benefit programs, maintaining back-office clerical support, and Human Resources information systems
 - a. Develop and administer programs related to medical, dental, vision, wellness, and life insurance. Such programs are reviewed annually to assess competitiveness and ensure cost effectiveness
 - b. Develop and administer compensation programs. Evaluate jobs to determine appropriate compensation levels and participate in market surveys to ensure compensation levels are fair and competitive as compared to similar roles in companies within the industry and companies with whom the Company competes for talent. Management compensation systems are reviewed annually and take into account economic conditions, wage trends, and market data. Wage rates for the union population are subject to collective bargaining
 - c. Administer and evaluate retirement programs including 401(k) and pension plans
 - d. Maintain the Human Resources information system of record and applicant tracking systems
2. Employee Relations is responsible for managing, addressing, and resolving employee concerns, as well as maintaining a positive relationship with the bargaining unit
 - a. Partner with functional areas to provide generalist support and consulting on a broad range of employee issues
 - b. Proactively identify potential employee or labor issues and work to resolve issues with employee or union when applicable
 - c. Ensure proper administration of Company labor agreements
3. Labor Relations is responsible for maintaining a positive relationship with the bargaining unit and managing the contract and negotiation processes
 - a. Manage the grievance, arbitration, and negotiation processes
4. Talent Management is responsible for assessing the people development needs of the organization and creating and executing appropriate training to meet those needs
 - a. Develop performance competencies and structure the performance review process. DP&L's annual performance evaluation process is included as Human Resources – Exhibit 2
 - b. Conduct talent dialogues to assess talent strengths and opportunities within each functional area
 - c. Develop the succession plan in conjunction with functional leadership
 - d. Assess developmental needs for individuals and functional areas and recommend, design, and/or deliver trainings to address identified gaps and needed productivity improvements

- e. Source and on-board new talent and ensure compliance to applicable local, state, and federal regulations and requirements
 - f. Develop and maintain campus recruitment strategies to include intern and co-op programs
 - g. Deliver and maintain employment testing programs to evaluate candidate capability
 - h. Participate in community outreach programs in support of the Company's diversity and inclusion strategy
5. Internal Communications is responsible for establishing a comprehensive internal communication plan and creating internal networks for building relationships
- a. Create and distribute Company communications such as electronic newsletters, printed materials, and email notices
 - b. Leverages relevant technology and tools to ensure our people receive timely & effective communication

The organizational chart for Human Resources is included as Human Resources - Exhibit 1.

Decision-Making and Control:

Human Resources' decision-making and control is achieved by individuals throughout the organization making decisions within their given scope of authority in support of the Company's overall mission and in accordance with the Company's policies and procedures. Decisions are raised to proper level of authority as required by Company policies. Overall responsibility for all decisions within the Human Resources function is that of the Vice President of Human Resources.

Performance against Human Resources goals are monitored on a continuous basis. This allows management to uncover trends in a timely manner and proactively address issues.

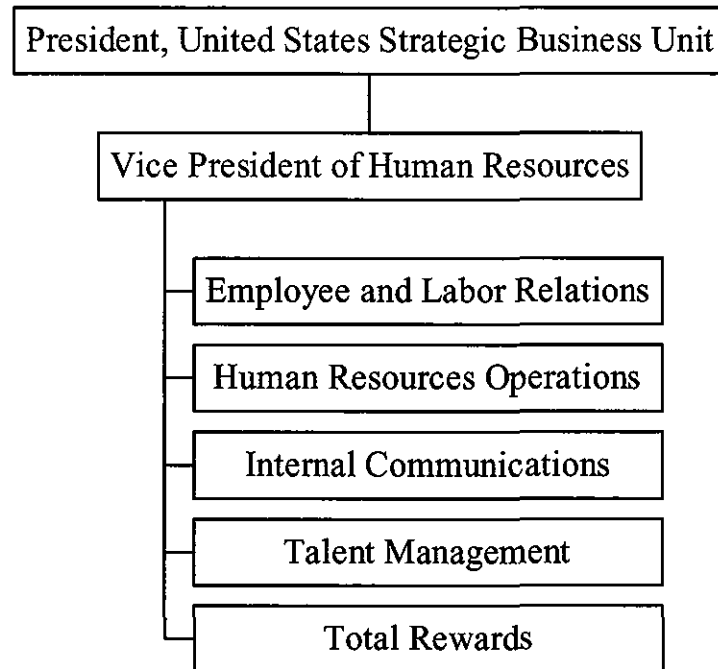
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including: face-to-face meetings, phone calls, conference calls and e-mail. Internal communications typically correspond to supporting the operations of other functional areas of the Company. These communications include providing information to all areas of the Company.

External communications are not typical for Human Resources related issues.

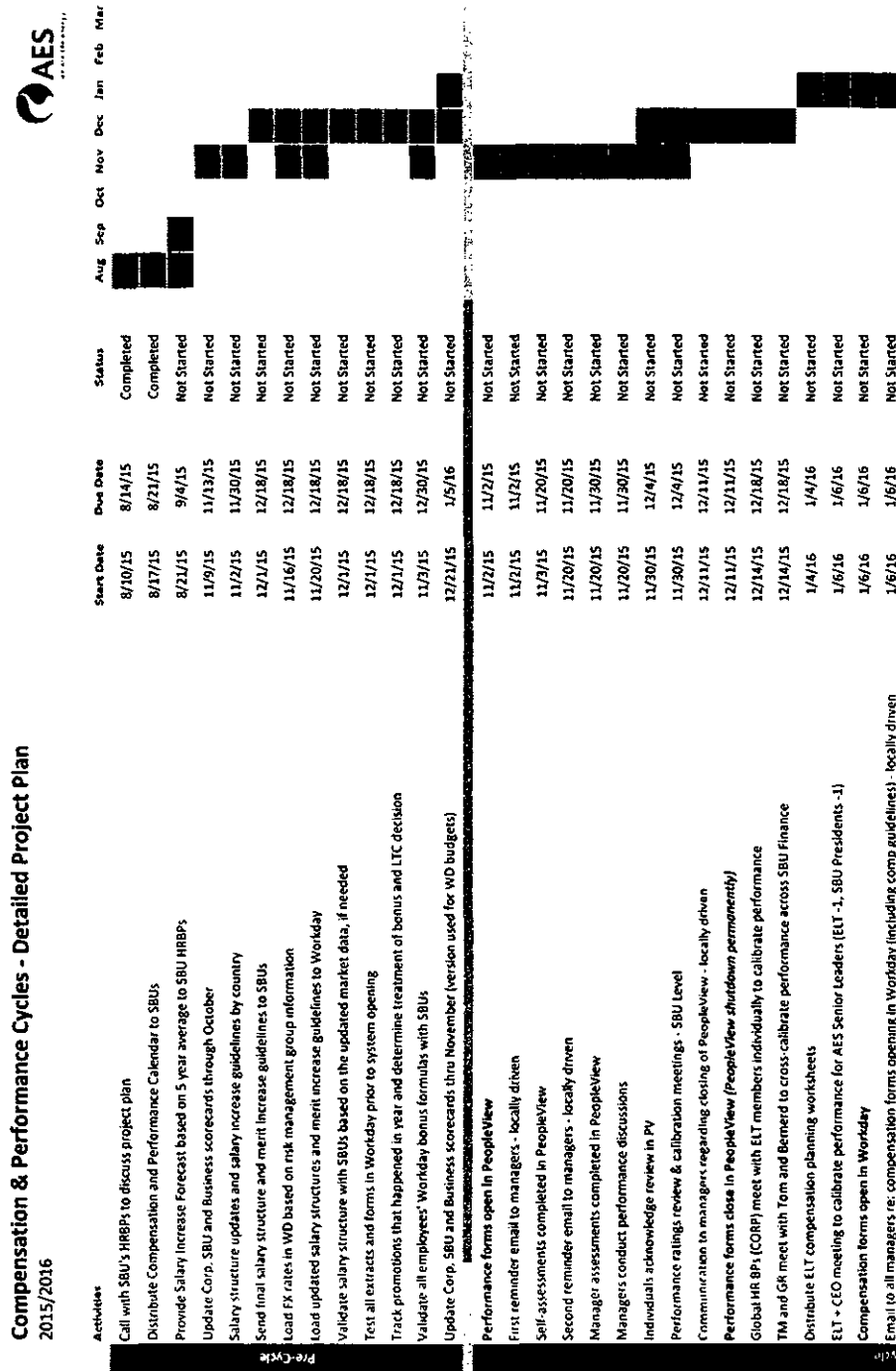
Human Resources - Exhibit 1

Organizational Chart for Human Resources



Human Resources - Exhibit 2

Annual Performance Evaluation Process

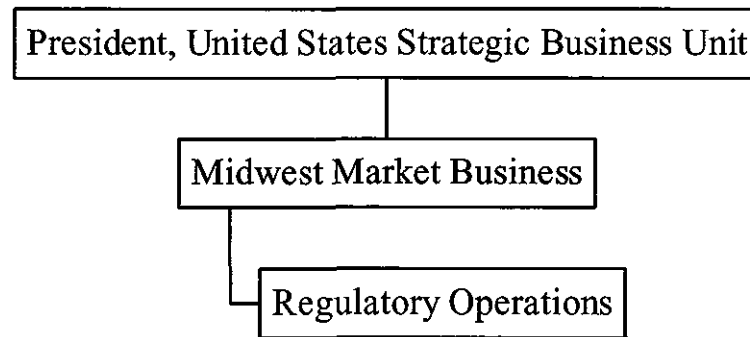


Compensation & Performance Cycles - Detailed Project Plan
2015/2016

| Compensation & Performance Cycles - Detailed Project Plan | | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar |
|--|--|------------|----------|-------------|-----|-----|-----|-----|-----|
| Activities | | Start Date | Due Date | Status | | | | | |
| Global HR BPs (CORP) meet with ELT members to input compensation recommendations in Workday | | 1/11/16 | 1/15/16 | Not Started | | | | | |
| First comp reminder email to managers - locally driven | | 1/18/16 | 1/18/16 | Not Started | | | | | |
| Send weekly aggregate report and status update to each country's HR contact + SBU HRBP | | 1/6/16 | 1/29/16 | Not Started | | | | | |
| Compensation forms closed in Workday | | 1/29/16 | 1/29/16 | Not Started | | | | | |
| CEO review of ELT direct reports and organizations | | 1/6/16 | 1/29/16 | Not Started | | | | | |
| Post System Close - Salary, Bonus and LTC Changes | | 1/30/16 | 2/12/16 | Not Started | | | | | |
| Global HR BPs (CORP) meet with ELT members to individually calibrate compensation | | 2/1/16 | 2/5/16 | Not Started | | | | | |
| TM GR & DF meet with Tom and Bernerd to cross-calibrate compensation across SBU finance | | 2/1/16 | 2/5/16 | Not Started | | | | | |
| ELT + CEO meeting to calibrate compensation for AES Senior Leaders (ELT - 3, SBU Presidents - 1) | | 2/18/16 | 2/18/16 | Not Started | | | | | |
| LTC grant review, reconciliation and approvals | | 2/15/16 | 2/16/16 | Not Started | | | | | |
| Compensation Committee meeting | | 2/18/16 | 2/18/16 | Not Started | | | | | |
| Reconcile Workday bonus amounts to corporate accrual | | 2/4/16 | 2/19/16 | Not Started | | | | | |
| Board of Directors meeting | | 2/19/16 | 2/19/16 | Not Started | | | | | |
| ELT grant communication | | 2/19/16 | 2/19/16 | Not Started | | | | | |
| Update Corp, SBU and Business scorecards based on full year | | 2/22/16 | 2/19/16 | Not Started | | | | | |
| Earliest date to communicate compensation and final overall performance rating | | 2/22/16 | 2/22/16 | Not Started | | | | | |
| Compensation worksheets for CEO, ELT and ELT direct reports | | 2/22/16 | 2/22/16 | Not Started | | | | | |
| Post System Close - Salary and Bonus Changes Only | | 2/18/16 | 2/26/16 | Not Started | | | | | |
| Email from CEO summarizing 2015 performance, payouts and profit sharing | | 2/22/16 | 2/22/16 | Not Started | | | | | |
| Managers communicate final performance ratings and compensation | | 2/23/16 | 2/26/16 | Not Started | | | | | |
| VP Total Rewards and CHRO Approve Salary and Bonus Recommendations | | 3/2/16 | 3/2/16 | Not Started | | | | | |
| New salary and incentive instructions from Workday to Payroll | | 3/2/16 | 3/2/16 | Not Started | | | | | |
| Email re: 401k contribution timing and bonus payouts | | 3/2/16 | 3/2/16 | Not Started | | | | | |
| 2016 Performance objectives and development goals entered in WPD | | 1/1/16 | 3/31/16 | Not Started | | | | | |

Midwest Market Business

Midwest Market Business is responsible for the overall development of business opportunities in the Midwest region. The Midwest region consists of the following states; Ohio, Indiana, Illinois, Iowa, Kansas, Kentucky, Michigan, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, Tennessee, Wisconsin and includes regulatory affairs in the State of Ohio. The DP&L specific functions are described in detail in the following section.



Functional Area:
Regulatory Operations

SFR Reference

- (B)(9)(c)(i) Identify the system or program for managing rate related operations and rate reform projects**
- (B)(9)(c)(ii) Rate program analytical process**
- (B)(9)(c)(iii) Implementation management**
- (B)(9)(c)(iv) Customer involvement**
- (B)(9)(c)(v) Commission and staff reporting**
- (B)(9)(i)(vii) Innovative rate and tariff processes, including analysis, design, implementation, and evaluation**

Policy and Goal Setting:

Regulatory Operations policies are put in place to generally ensure the Company is in compliance with federal, state and local regulations and policies. DP&L's policies are developed by DP&L's management under the guidance of AES's management and AES's board of directors. All parties are equally responsible to ensure that DP&L policies meet or exceed the requirements set forth by all of DP&L's regulating entities.

Regulatory Operations establishes the policy by which the rates and regulated tariff sheets for DP&L are administered and implemented. A primary function of Regulatory Operations is to act as a liaison between the PUCO, the FERC, and the Office of Ohio Consumers' Counsel and the Company. All information shared with these entities is coordinated through Regulatory Operations.

The top priority of all DP&L departments is to ensure the safety of all DP&L employees, contractors and the public. Regulatory Operations takes this priority seriously, and incorporates safety into all aspects of operations. Safety meetings are held once a month to further educate employees on not only safety at work, but also taking safety home.

Regulatory Operations' goals are developed to align with the Midwest Market Business Leader's objectives, which fully support Company and Corporate goals, set by AES's management and board of directors.

Strategic and Long-Range Planning:

The Regulatory Operations Department reflects DP&L's long-range strategy to achieve DP&L's goal of delivering safe, reliable service at a fair price to customers to meet compliance and reliability targets as well as our customers' needs. DP&L's Financial Planning and Analysis Department sets a 10-year long-term financial budget by which actual data is measured and analyzed. One of Regulatory Operations' responsibilities is to assess the timing and need for rate cases by comparing this 10-year budget with the 10-year rate and revenue forecast. Regulatory Operations provides the forecasted rates to Financial Planning to develop a long-term outlook on

utility revenue. Need and timing of rate cases is determined based on the regulatory environment, planned projects, and a review of actual and budgeted financials, including an analysis of current return on equity.

Organizational Structure and Responsibilities:

The Regulatory Operations Department consists of 7 rate analysts who are led by 2 regulatory managers. Regulatory Operations is supported by nearly all functional areas of the company including; Legal, Accounting, Tax, Financial Planning and Analysis, and Customer Service System and Information Technology.

Regulatory Operations has responsibility for and manages the objective of DP&L's rate related operations, to ensure the Company has the financial stability to maintain safe and reliable service and to ensure all customers are paying their fair share of rates based on cost causation principles, by the following actions:

1. Analyze the need for cost recovery and/or compliance filings at both the PUCO and FERC. The analytical process is as follows:
 - a. Monitor and review other Ohio utility rates, programs, and filings, along with national utility pricing and regulatory issues to evaluate the impact to DP&L. In addition, rate and revenue forecasts are developed and compared along with the Company's forecast of expenses, infrastructure investment, and depreciation rates to determine the financial health of the regulated utility and ensure that the objectives of the current rates are being met
 - b. Periodically review DP&L's tariff terms and conditions to ensure Customer Operations personnel are providing service in a cost effective and efficient way and that is consistent with tariff terms and conditions as well as the O.A.C. Changes in technology, Company policies, or PUCO policies at times trigger review of tariff terms and conditions by both Regulatory Operations and Customer Operations. Regulatory Operations evaluates any recommendations from Customer Operations to determine if tariff updates are needed
 - c. Perform analysis of new or increasing costs incurred by DP&L in order to ensure appropriate recovery measures for regulated costs. Internal meetings are initiated with Accounting, Tax and other internal areas to conduct this analysis
 - d. Analysis of customer benefits as regulated projects are being deliberated internally and at the PUCO or FERC. Analysis includes looking at the customer benefits including; customer satisfaction, rate impact, and operation and maintenance savings
 - e. Regulatory Operations utilizes various information technology systems including; Oracle, Discoverer, and DP&L's customer information system (billing system). These systems support the area in resolving issues and developing revenue requirements

2. Direct the preparation of rate applications and coordinate all aspects of rate proceedings before the PUCO and/or FERC. Regulatory Operations develops various other state and federal regulatory filings and ensures these filings comply with local, state, and federal policies and laws

Other responsibilities of Regulatory Operations include:

1. Implementation of rate-related Commission Orders
2. Test rate changes to ensure customer bills are produced accurately
3. Develop typical customer bill analysis to ensure no specific groups of customers are being unfairly burdened by new rate designs
4. Evaluate legislative initiatives and the impact to customer rates, service and Company cost recovery should these new laws be enacted
5. Provide call center training and prepare frequently asked questions document for any new rates established by DP&L
6. Work with Corporate Communications to respond to any media requests relating to rates, regulations, and PUCO or FERC decisions or rulemakings
7. Develop bill messages and inserts to be sent to customers monthly, quarterly, annually, or on a periodic basis
8. Create and evaluate possible alternative and innovative rate structures
9. Work with the PUCO Staff on customer complaint inquiries
10. Provide data and information to various governmental and industry parties in the form of rate surveys and other industry information requests

A listing of standards and other reference materials utilized by Regulatory Operations is included as Regulatory Operations – Exhibit 2.

Significant projects in progress:

1. Electric Security Plan II – Final implementation of the Commission’s Opinion and Order, including the transition to 100% competitively bid generation starting January 1, 2016
2. Bill Format Redesign – Implementation of a new, modern bill format with the inclusion of CRES Provider logos
3. Energy Efficiency Portfolio Plan – Probable 2016 filing to set DP&L’s energy efficiency program for the years 2017 through 2019

The organizational chart for Regulatory Operations is included as Regulatory Operations – Exhibit 1.

Decision-Making and Control:

Regulatory Operations decision-making and control is achieved by individuals throughout the organization making decisions within their given scope of authority in support of DP&L’s overall mission and in accordance with the DP&L policies and procedures. Decisions are raised to proper level of authority as required by DP&L’s policies. Overall responsibility for all

Regulatory Operations decisions is that of the AES US SBU, Market Business Leader for the Midwest region.

Performance against the Regulatory Operations goals is monitored and reported on a continuous basis, which includes monitoring of budgets, compliance, and how DP&L's rates compare with those of the other Ohio utilities. This monitoring helps to ensure that the objectives of the rates are meeting the needs of the customers and the Company. This allows management to uncover trends in a timely manner and proactively address issues.

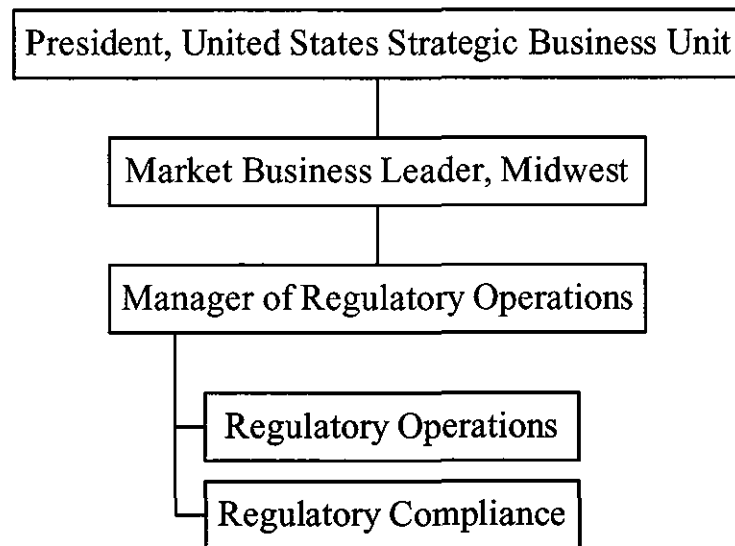
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including: phone calls, conference calls, face-to-face meetings, and e-mail. Internal communications typically relate to inquiries of other functional units, specifically; Customer Operations, Accounting, Tax, and Customer Service System. Regulatory Operations conveys issues to these groups in order to receive feedback and support for filings, along with requesting comments pertaining to overall policy and compliance reasons. Additionally, Regulatory Operations holds internal team meetings on a periodic basis to ensure all analysts and managers stay up to date on current issues and to brainstorm new and innovative ideas.

External communications are accomplished through a variety of communication channels including: phone calls, face-to-face meetings, and e-mail. Direct external communications can be extensive and the result of rate case public hearings and notifications, case settlement, PUCO inquiries and data requests, third parties, and sometimes customer inquiries. There are also a few indirect methods for customers and other parties to communicate with DP&L regarding rates and/or tariffs. One of the primary ways Regulatory Operations communicates its rates and policies externally is by including them on the DP&L website which includes tariffs, a price-to-compare calculator, and a list of registered CRES Providers.

Regulatory Operations - Exhibit 1

Organizational Chart for Regulatory Operations



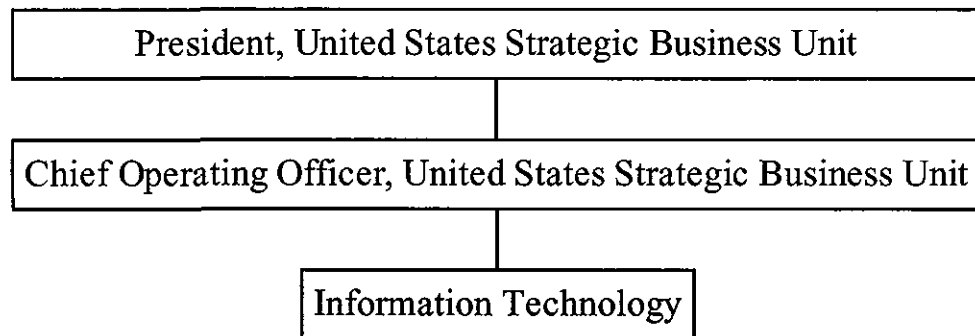
Regulatory Operations - Exhibit 2

List of Standards and Pertinent Reference Materials

- DP&L Tariffs – PUCO No. 17
- Ohio Revised Code
- Ohio Administrative Code
- Bill Calculators
- Bill Calculator Guides
- DP&L's Electric Security Plan II Commission Order
- DP&L's Energy Efficiency Portfolio Stipulation

Information Technology

Information Technology is responsible for the DP&L hardware, software and web activities. The Information Technology specific functions are described in detail in the following section.



Functional Area:
Information Technology

SFR Reference

- (B)(9)(f)(i) Description of major systems and platforms utilized by the company including capital and human resources allocated to each system/platform**
- (B)(9)(f)(ii) Corporate plans for major systems, (development, integration, and retirement)**
- (B)(9)(f)(iii) Policies for protecting company and customer information/data**
- (B)(9) Staff Letter**

Policy and Goal Setting:

DP&L's Information Technology policies are driven by regulatory requirements, legal guidelines and the overarching governance related to the availability, acceptable use and protection of Company data and technology assets. As part of the US SBU shared services, the Information Technology group develops and enforces policies that meet the needs of DP&L and its employees. Policies are developed by Information Technology management under the guidance of DP&L and AES's management and board of directors. All parties are equally responsible to ensure that DP&L policies meet or exceed the requirements set forth by all of DP&L's regulating entities.

Information Technology policies and general controls are meant to provide direction on the use of Company sanctioned technology and associated data so that assets and information (Company and customer) are protected. Information Technology general controls ensure that proper policies, procedures and documentation exist and are followed. They are in place to verify the development and implementation of applications, as well as the integrity of applications and data, and operations are performed as defined and as expected. As such, these policies span many areas, including but not limited to:

1. Acceptable use
2. Remote access
3. E-mail and instant messaging
4. Access control
5. Internet use and monitoring
6. Anti-virus
7. Network and wireless security

DP&L Information Technology policies can be found in Information Technology - Exhibit 2. Additional Information Technology related policies are documented and maintained by the Physical Security and Cyber Security teams at DP&L.

Guidelines are in place for each policy to be reviewed and updated as necessary.

Goal setting for Information Technology is a function of several drivers. The annual capital budgeting process identifies company initiatives that will require technology delivery and

Information Technology support. The initiatives translate directly into goals for the Information Technology organization. In addition, periodic work and tasks are identified in the interest of maintaining the Information Technology systems portfolio and ensuring general availability. Lastly, Information Technology goals stem from commitments to the strategy and mission of the company. These include goals pertaining to safety, compliance, reliability, and budgets.

Strategic and Long-Range Planning:

Long-range and strategic planning in Information Technology is aligned with similar activities within DP&L and AES. Each year a ten year projection is created and submitted that reflects the anticipated needs and associated budgetary requirements for that time period. This represents the strategic needs, portfolio maintenance requirements and technology commitments to internal and external entities. Planning documents typically address the budgetary and staffing requirements to achieve specific needs based on Company strategy. Information Technology - Exhibit 3 is a list of the Information Technology capital initiatives planned for 2016.

The Information Technology mission statement guides the actions of the Information Technology organization and calls out the overall goals, included as Information Technology – Exhibit 4. An Information Technology business plan exists to align with the overall business plan for the US SBU. The current Information Technology business plan addresses goals in five major areas:

1. Operational excellence
2. Financial excellence
3. People
4. Growth
5. Customer market facing

Information Technology maintains various technology roadmaps which assist in providing a big picture of future plans for major systems. Development, integration and retirement of Information Technology systems are all considered as part of the roadmaps. The Information Technology transformation roadmap is included as Information Technology – Exhibit 5.

The majority of the Information Technology platforms used by the company include Microsoft Windows operating systems, Unix and Linux operating systems, IBM mainframe operating system, and Microsoft SQL, Oracle and IBM DB2 databases.

Organizational Structure and Responsibilities:

The Information Technology organization is part of the US SBU. It exists to serve all interests of US SBU companies and entities, including DP&L. It is led by the Director of Information Technology and is comprised of 7 distinct technology areas as illustrated in Information – Technology – Table 1.

Information Technology – Table 1

| Technology Area | Description | Key Applications / Systems |
|---|---|---|
| 1. Enterprise Applications | Implements and maintains systems that serve the entire company | <ul style="list-style-type: none"> • Oracle e-Business Suite (ERP) for financial and supply chain management, analytics and reporting • Human Resources and Payroll • Governance, risk management, and compliance • Application Integrations |
| 2. Generation Applications | Supports all applications that serve the power generation facilities of the company | <ul style="list-style-type: none"> • Work and asset management • Asset performance management • Fuel management • Lock out – tag out • SCADA and associated control systems |
| 3. Transmission and Distribution Applications | Supports the operational technology used in transmission and distribution operations | <ul style="list-style-type: none"> • Geographic Information Systems • Outage management • Metering systems • Work management • Substation maintenance • Customer support systems for call center, customer operations and billing |
| 4. Data Center | Implements and maintains the underlying infrastructure to support all other Information Technology functions and business computing needs | <ul style="list-style-type: none"> • Servers and storage • Mainframe computing • Data Center facilities |
| 5. Telecommunications | Implements and maintains the telecommunications capability to support all technology and business needs | <ul style="list-style-type: none"> • Networks • Internet connectivity • Physical Plant • Telecommunications (voice, video) |
| 6. Collaboration | Delivers and manages tools required for effective work collaboration and productivity across the enterprise | <ul style="list-style-type: none"> • Account and e-mail administration • Information Technology service desk • Information Technology field personal computer services • Information Technology asset management • Desktop software engineering • Cell phone administration • Collaboration tools (instant messaging, video and voice) |
| 7. Governance | Provides oversight for the other Information Technology groups | <ul style="list-style-type: none"> • Policies and general controls • Project management • Capital project approval and tracking • Technical architecture • Budget support • Information Technology audit and risk management • Key performance indicator tracking and reporting |

Each of these groups work toward common goals while focusing in their respective specialty areas to deliver the technology and services required for company growth and success.

The Information Technology organization is comprised of 123 individuals who serve in various capacities including managers, team leads, analysts, engineers, project managers, administrators and architects. These resources work together on the ideation, delivery & support of the technology that makes up the Information Technology systems portfolio for the entire US SBU. The Director of Information Technology reports to the US SBU Chief Operating Officer.

A brief description of systems supported by each group is available in Information Technology – Exhibit 6. The Information Technology organizational chart is included as Information Technology – Exhibit 1.

Decision-Making and Control:

In large part, decision-making and control subscribes to the traditional hierarchical management structure described above. Policies and procedures for Information Technology, as well as DP&L and AES also govern decision-making and the associated control. Additionally, workflow and technology is used to enforce financial approvals and other decisions that require certain degrees of approval authority. Overall responsibility for decisions in Information Technology resides with the Director of Information Technology.

Performance against Information Technology commitments are tracked via KPIs and published monthly in a visual scorecard format. These KPIs cover key aspects of the work Information Technology does to support the work of the company including safety, work backlog, customer call center system availability, critical systems availability, project status, change management and budget performance.

Internal and External Communications:

Internal communications involve communications between Information Technology and the business areas that subscribe to Information Technology services. Specific Information Technology individuals are responsible for business relationship management within strategic areas of the business providing opportunities to review business priorities and plans. Methods of communication include:

1. Face-to-face communication in meetings and individual conversations
2. Phone calls, conference calls and videoconferencing
3. Email
4. Instant messaging
5. Publication and dissemination of written materials

These internal communications are used to update, educate, clarify and generally ensure the understanding of business matters internal to DP&L.

External communications involve communications with outside entities and are accomplished using the same methods listed. Examples of external entities include customers, regulatory groups, suppliers, service providers and government representatives.

Staff Letter

Dayton Power and Light shall provide the Standard Filing Requirements (SFR) information relating to corporate plans and planning for major systems, (development, integration, and retirement) pursuant to Ohio Administrative Code 4901-7, Chapter II, Appendix A, (B)(9)(f), as well as provide information related specifically to the planning assessment of the ability of existing billing system(s) and/or customer information system(s) to accommodate meter information from AMI/smart meter deployment and customer energy usage data to competitive electric supply providers, pursuant to Ohio Administrative Code 4901-7, Chapter II, Appendix A, (B)(9)(f) (ii) and (iii).

DP&L's customer service system is a mainframe billing system that was developed by DP&L resources. It leverages the former Arthur Andersen utilities billing platform, Customer/1. The customer service system is a highly customized system and is compliant with all regulations. The system has received many enhancements since its inception, to comply with regulatory changes as well as to continually improve its performance. These enhancements have included initiatives that support customer choice such as rate-ready billing, bill-ready billing, and percentage off price-to-compare pricing. A timeline listing of some of the most recent enhancements is included as Information Technology – Exhibit 7. The result of these enhancements is a highly customized customer service system that continues to be flexible enough to adapt to changing billing needs and requirements and continues to maintain compliance with all regulations.

DP&L plans to evaluate the prudence of continued use of the existing customer service system beginning in 2017 with the development of system requirements followed by the distribution of a request for proposal. This process will identify both the capabilities and cost for implementing a commercially available billing system. In making the decision whether to continue to support and enhance the existing customer service system or to implement a new billing system, DP&L will evaluate the following criteria:

1. Technical capabilities of the existing customer service system versus the commercially available billing systems
2. Projected compliance capability of the customer service system
3. Projected compliance capability and required customizations for a new billing system
4. Operational benefits of a new billing system
5. Customer benefits of a new billing system
6. Supplier benefits of a new billing system
7. Total lifecycle cost of implementing a new billing system

DP&L currently operates an Internet portal for CRES providers, which is available at <https://cres.dpandl.com>. It contains public information such as aggregate load profiles, registration materials, the supplier handbook, and frequently asked questions. From this portal, CRES providers can gain access to additional information via a secure log-in and password. This additional information includes the standard pre-enrollment customer list and access to 24-month historical summary usage data by account number. Further, CRES providers

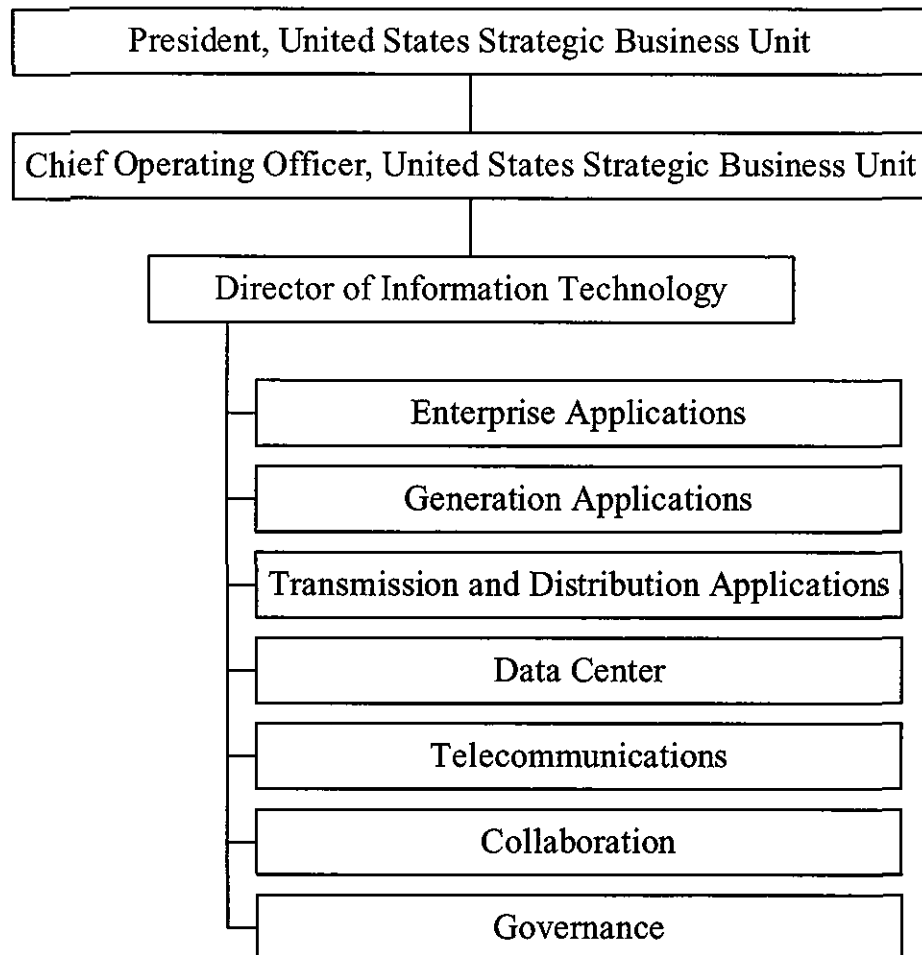
that are registered suppliers for DP&L have access to information specific to their customers such as a list of active accounts. CRES providers may also request interval data by account number via Electronic Data Interchange (EDI). DP&L currently has interval data for approximately 2,500 non-residential customers. An image of the CRES portal home page is included as Information Technology – Exhibit 8.

As DP&L develops its plans for a Smart Grid, it will include as one of its basic requirements continuing to supply CRES providers with the same information that they have access to today. In addition, DP&L will supply CRES providers with interval data for all customers with AMI, including both residential and non-residential customers. DP&L is working toward providing at least hourly level data to all retail suppliers. This information will continue to be transmitted via EDI, or CRES providers will be able to access the data directly through the portal. For residential customers, CRES providers will be required to submit a letter of authorization, in compliance with PUCO rules, via the portal in order to receive the residential customer interval data. The letter of authorization will then be validated and maintained by DP&L. As a final note, DP&L will comply with future requirements related to information exchange with CRES providers and the retailer portal, as those requirements are further defined by the PUCO.

The customer service system is integrated with many of DP&L's existing systems, including MV-90, CRES provider and customer internet portals, and the Oracle general ledger. A listing of the various functions and systems integrated with the customer service system is included as Information Technology – Exhibit 9. As with other integrated technologies, at the time when DP&L implements a Smart Grid/Automated Metering Infrastructure ("AMI") plan, there will be new capabilities that cannot be performed by existing systems that will require a number of new systems and applications. A primary example is meter data management. As we envision an AMI deployment, the customer service system will be able to interface with the new meter data management system ("MDMS"), as it will be a core repository for the type and quantity of meter data from the two-way meters. Thus, while the customer service system will not be required to store or account for the additional meter information, it will need to have an interface configured to accept data such as billing determinants for each meter and customer account. Such an interface will be comparable to the existing interface between the customer service system and MV-90, DP&L's current interval meter data repository. Similarly, appropriate access to information from the MDMS can be developed and offered to the CRES providers via the supplier portal.

Information Technology – Exhibit 1

Organizational chart for Information Technology



Information Technology – Exhibit 2

Information Technology Policies



AES US Strategic Business Unit (“US SBU”)

Information Technology Operating Policies

***US SBU SYSTEMS AND APPLICATION BACKUP
AND RECOVERY POLICY***

Policy Owner: US SBU Information Technology - Governance

Original issue Date: 05/26/2015

US SBU SYSTEMS AND APPLICATION BACKUP POLICY

Contents

| | | |
|------------|--|----------|
| 1.0 | Introduction..... | 1 |
| 2.0 | Scope | 1 |
| 3.0 | Definitions | 1 |
| 3.1 | Backup Catalog..... | 1 |
| 3.2 | Development Data..... | 1 |
| 3.3 | Production Data | 1 |
| 3.4 | Scheduled Changes..... | 1 |
| 4.0 | Systems and Applications Backup | 2 |
| 4.1 | Backups | 2 |
| 4.2 | Logging and Monitoring..... | 2 |
| 4.3 | Catalog | 2 |
| 4.4 | Recovery Testing and Review | 2 |
| 4.5 | Retention and Review..... | 2 |
| 5.0 | APPROVALS..... | 3 |
| 6.0 | Version Control History..... | 4 |

| |
|--|
| Document Control No.: IT-001 Last Revised Date: 5-12-2015 Page 1 |
|--|

US SBU SYSTEMS AND APPLICATION BACKUP POLICY

1.0 Introduction

This policy ensures that production and development data is protected from intentional or unintentional destruction that may impact the integrity and / or availability of US SBU operations.

2.0 Scope

This policy is applicable to AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, and any affiliate of US Services that adopts this policy pursuant to its own corporate governance procedures (collectively, the "Companies"). Documentation of adoption of this policy by a US Services affiliate shall be kept by the US Services Policy Committee or it's designate. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp.

3.0 Definitions

3.1 Backup Catalog

The catalog stores information regarding backups. The Catalog typically keeps track of the resources, files, etc., that are backed up, along with times and dates and which media, tape or disk folders where the backed up data is stored. The Catalog effectively serves as the table of contents for the backup system.

3.2 Development Data

All information stored on US SBU computer infrastructure (Servers) used for quality assurance, testing, and development purposes.

3.3 Production Data

All information stored on US SBU computer infrastructure (servers) used to run the business. This includes Operating Systems, applications, and data for the production environment. This policy does not cover information stored on personal computers.

3.4 Scheduled Changes

Any change to a standing server backup schedule in either frequency or scope excluding new servers or servers that are being decommissioned.

| |
|--|
| Document Control No.: IT-001 Last Revised Date: 5-12-2015 Page 2 |
|--|

US SBU SYSTEMS AND APPLICATION BACKUP POLICY

4.0 Systems and Applications Backup

4.1 Backups

Backups must be performed in a manner that allows the US SBU to meet their recovery point objectives (RPO).

4.2 Logging and Monitoring

All executed backups will be logged and monitored.

4.3 Catalog

A backup catalog must be used for media tracking and storage.

4.4 Recovery Testing and Review

Samples of data must be recovered and validated to make sure the backup system is functioning correctly. Testing must be logged and the logs retained according to prevailing retention policy, or any legal requirements.

4.5 Retention and Review

All backup media of applications, systems and data must be retained according to prevailing retention policy or any applicable legal requirements.

The review should be formally documented and retained with the local backup procedure.


Document Control No.: **IT-001**
Last Revised Date: 5-12-2015
Page 3

US SBU SYSTEMS AND APPLICATION BACKUP POLICY

5.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:

| | |
|--|----------------|
|  Mike Collier - US SBU IT Director | 7/1/15 Date |
|--|----------------|

Document Control No. IT-001
Last Revised Date: 5-12-2015
Page 4

US SBU SYSTEMS AND APPLICATION BACKUP POLICY

6.0 Version Control History

| Date | Description of Changes | Author(s) | Approver(s) |
|--------------|-------------------------------|-------------------------------|--------------------|
| May 12, 2015 | Initial Policy creation | IT Governance Mike Gardner | |
| | | | |
| | | | |



AES US Strategic Business Unit ("US SBU")

Information Technology Operating Policies

US SBU Change Management POLICY

Policy Owner: US SBU Information Technology - Governance

Original Issue Date: 05/29/2015

US SBU CHANGE MANAGEMENT POLICY

Contents

| | | |
|-----|----------------------------------|---|
| 1.0 | Introduction | 1 |
| 2.0 | Scope | 1 |
| 3.0 | Definitions | 1 |
| 3.1 | Change Control | 1 |
| 3.2 | Change Management | 1 |
| 3.3 | Custodian | 1 |
| 4.0 | Policy | 2 |
| 4.1 | Establish Process | 2 |
| 4.2 | Tracking System | 2 |
| 4.3 | Testing | 2 |
| 4.4 | Back Out and Recovery Plan | 2 |
| 4.5 | Authorized Approval | 2 |
| 4.6 | Segregation of Duties | 2 |
| 4.7 | Review | 2 |
| 5.0 | APPROVALS | 3 |
| 6.0 | Version Control History | 4 |

| |
|---|
| Document Control No.: IT-002 Last Revised Date: 5-13-2015 Page 1 |
|---|

US SBU CHANGE MANAGEMENT POLICY

1.0 Introduction

This policy mandates that changes to critical systems, applications, and data follow a stringent change management approval process.

2.0 Scope

This policy is applicable to AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, and any affiliate of US Services that adopts this policy pursuant to its own corporate governance procedures (collectively, the "Companies"). Documentation of adoption of this policy by a US Services affiliate shall be kept by the US Services Policy Committee or its designate. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp.

3.0 Definitions

3.1 Change Control

The procedures to ensure that all changes are controlled, including the submission, recording, analysis, decision making, and approval of the change

3.2 Change Management

The Service Management process responsible for controlling and managing requests to effect changes to the IT Infrastructure, or any aspect of IT services, to promote business benefit while minimizing the risk of disruption to services

3.3 Custodian

Individuals with the authority to approve changes to production environments

| |
|---|
| Document Control No.: IT-002 Last Revised Date: 5-13-2015 Page 2 |
|---|

US SBU CHANGE MANAGEMENT POLICY

4.0 Policy

4.1 Establish Process

A change control and configuration management process shall be established, documented, and utilized for adding, modifying, replacing, or removing hardware, applications or data.

4.2 Tracking System

A change request tracking system must be utilized to initiate and document all changes, including emergency changes for each request.

4.3 Testing

All changes to US SBU systems must be tested and the documentation must be retained based on local or corporate retention policy. Changes to US SBU systems must be developed and tested in physically or logically segregated environment(s), separate from the production environment.

4.4 Back Out and Recovery Plan

Back-out and recovery plans must be documented and approved. Documentation must be retained based on local or corporate retention policy.

4.5 Authorized Approval

Business and IT custodians will be identified and documented in an approval matrix. This approval matrix will be maintained as needed. These custodians will review and authorize change requests according to their responsibilities prior to implementation to the production environment. These changes and authorizations must be documented using an IT Change Request form. Documentation must be retained based on local or corporate retention policy.

4.6 Segregation of Duties

Segregation of duties shall exist between the roles identified in the process. Programmers/Developers must not have functional access to the production environment.

4.7 Review

The change control process and the custodian responsibilities are reviewed and monitored to ensure all process controls operate as intended.

Document Control No.: IT-002
Last Revised Date: 5-13-2015
Page 3

US SBU CHANGE MANAGEMENT POLICY

5.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:

| | |
|--|----------------|
|  Mike Collier – US SBU IT Director | 7/1/15 Date |
|--|----------------|

Document Control No.: **IT-002**
Last Revised Date: 5-13-2015
Page 4

US SBU CHANGE MANAGEMENT POLICY

6.0 Version Control History

| Date | Description of Changes | Author(s) | Approver(s) |
|--------------|-------------------------------|------------------|--------------------|
| May 14, 2015 | Initial Policy creation | IT Governance | |
| | | | |
| | | | |



AES US Strategic Business Unit ("US SBU")

Information Technology Operating Policies

US SBU JOB AND BATCH SCHEDULING POLICY

Policy Owner: US SBU Information Technology - Governance

Original issue Date: 05/29 /2015

Revision Date: n/a

US SBU JOB AND BATCH SCHEDULING POLICY

Contents

| | | |
|------------|---|----------|
| 1.0 | Introduction..... | 1 |
| 2.0 | Scope | 1 |
| 3.0 | Definition(s)..... | 1 |
| 3.1 | Batch and Job Scheduling..... | 1 |
| 4.0 | Job and Batch Scheduling..... | 2 |
| 4.1 | Critical Jobs List | 2 |
| 4.2 | Job and Batch Scheduler access | 2 |
| 4.3 | Logging..... | 2 |
| 4.4 | Monitoring/Failure Handling..... | 2 |
| 4.5 | Review | 2 |
| 5.0 | APPROVALS..... | 3 |
| 6.0 | Version Control History..... | 4 |

| |
|---|
| <i>Document Control No.: IT-003</i> <i>Last Revised Date: 5-12-2015</i> <i>Page 1</i> |
|---|

US SBU JOB AND BATCH SCHEDULING POLICY

1.0 Introduction

This policy ensures that production and development data is protected from intentional or unintentional destruction that may impact the integrity and / or availability of US SBU operations.

The objective of this document is to define job processing as a critical IT operational control. Effective operational controls ensure automated procedures are executed as designed, and that errors and incidents are promptly addressed

2.0 Scope

This policy is applicable to AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, and any affiliate of US Services that adopts this policy pursuant to its own corporate governance procedures (collectively, the "Companies"). Documentation of adoption of this policy by a US Services affiliate shall be kept by the US Services Policy Committee or its designate. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp.

3.0 Definition(s)

3.1 Batch and Job Scheduling

A computer application for controlling unattended background program execution (commonly called batch processing)

| |
|---|
| <i>Document Control No.: IT-003</i> <i>Last Revised Date: 5-12-2015</i> <i>Page 2</i> |
|---|

US SBU JOB AND BATCH SCHEDULING POLICY

4.0 *Job and Batch Scheduling*

4.1 *Critical Jobs List*

A list of critical scheduled jobs and batch activities must be created and maintained.

4.2 *Job and Batch Scheduler access*

Access to create, modify and delete critical scheduled jobs and batch activities must be authorized.

4.3 *Logging*

All critical scheduled jobs and batch activities must be logged.

4.4 *Monitoring/Failure Handling*

Failures in the execution of a critical scheduled job(s) or batch activity must be documented and resolved appropriately.

4.5 *Review*

The logs of critical scheduled jobs and batch activities must be reviewed.

This review must be formally documented and retained.

Document Control No.: IT-003
Last Revised Date: 5-12-2015
Page 3

US SBU JOB AND BATCH SCHEDULING POLICY

5.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:

| | |
|--|----------------|
|  Mike Collier – US SBU IT Director | 7/1/15 Date |
|--|----------------|

Document Control No.: IT-003
Last Revised Date: 5.12.2015
Page 4

US SBU JOB AND BATCH SCHEDULING POLICY

6.0 Version Control History

| <i>Date</i> | <i>Description of Changes</i> | <i>Author(s)</i> | <i>Approver(s)</i> |
|--------------|-------------------------------|-------------------------------|--------------------|
| May 12, 2015 | Initial Policy creation | IT Governance Mike Gardner | |
| | | | |
| | | | |



AES US Strategic Business Unit (“US SBU”)

Information Technology Operating Policies

US SBU PROGRAM DEVELOPMENT POLICY

Policy Owner: US SBU Information Technology - Governance

Original Issue Date: 05/29/2015

Revision Date: n/a

US SBU PROGRAM DEVELOPMENT POLICY

Contents

| | | |
|------------|---|----------|
| 1.0 | Introduction..... | 1 |
| 2.0 | Scope | 1 |
| 3.0 | Definitions | 1 |
| 3.1 | SOC Reports | 1 |
| 4.0 | Program Development Policy..... | 2 |
| 4.1 | Ensure Business and AES Strategy Alignment | 2 |
| 4.2 | Assess Risks..... | 2 |
| 4.3 | Document and Test | 2 |
| 4.4 | Training and Communications | 2 |
| 4.5 | Third Party Providers | 2 |
| 5.0 | APPROVALS..... | 3 |
| 6.0 | Version Control History..... | 4 |

| |
|--|
| Document Control No.: 17-004 Last Revised Date: 5-21-2015 Page 1 |
|--|

US SBU PROGRAM DEVELOPMENT POLICY

1.0 *Introduction*

This policy mandates that new US SBU systems or changes to existing US SBU systems (whether hosted internally or outsourced) support the operations of US SBU businesses by requiring that they are aligned with business objectives, authorized, and tested.

2.0 *Scope*

This policy is applicable to AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, and any affiliate of US Services that adopts this policy pursuant to its own corporate governance procedures (collectively, the "Companies"). Documentation of adoption of this policy by a US Services affiliate shall be kept by the US Services Policy Committee or it's designate. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp.

3.0 *Definitions*

3.1 *SOC Reports*

Service Organization Control Reports* are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service

SOC 1: Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting Guide

SOC 2: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

| |
|--|
| Document Control No.: IT-004 Last Revised Date: 5-21-2015 Page 2 |
|--|

US SBU PROGRAM DEVELOPMENT POLICY

4.0 Program Development Policy

4.1 Ensure Business and AES Strategy Alignment

Ensure business owners within the US SBU participate in, and approve, the selection and design of new systems to ensure they meet business requirements prior to the execution of a new project. In addition, document technology and business management approval by following the Change Management Policy prior to final go-live of any new US SBU systems or projects.

Measures must also be taken to evaluate if the new critical initiatives impact AES corporate strategies and if so, ensure that the initiative is strategically aligned with AES strategy and that appropriate AES approvals are gathered.

4.2 Assess Risks

Facilitate a risk assessment to ensure the successful implementation of the activity.

4.3 Document and Test

Create system support, training, and user documentation as necessary for all newly developed or acquired systems.

Develop, document, and execute test strategies for US SBU systems being developed or acquired, based on the risk of the implementation to the US SBU.

4.4 Training and Communications

Available training and documentation must be communicated to end users and support personnel.

4.5 Third Party Providers

Based on the risk to the US SBU, ensure that third party providers perform independent reviews of the IT Services performed by an outsourced provider on behalf of the US SBU and produce an annual independent audit report (i.e. SOC 1, SOC 2), or allow the US SBU the "right to audit". Ensure that US SBU management reviews and assesses this report on an annual basis and determines if risks are appropriately mitigated.

Document Control No.: IT-004
Last Revised Date: 5-21-2015
Page 3

US SBU PROGRAM DEVELOPMENT POLICY

5.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:

| | |
|--|----------------|
|  Mike Collier - US SBU IT Director | 7/1/15 Date |
|--|----------------|

Document Control No. IT-004
Last Revised Date: 5-21-2015
Page 4

US SBU PROGRAM DEVELOPMENT POLICY

6.0 Version Control History

| <i>Date</i> | <i>Description of Changes</i> | <i>Author(s)</i> | <i>Approver(s)</i> |
|---------------------|--------------------------------|---------------------------------------|--------------------|
| <i>May 21, 2015</i> | <i>Initial Policy creation</i> | <i>IT Governance Mike Gardner</i> | |
| | | | |
| | | | |



AES US Strategic Business Unit ("US SBU")

Information Technology Operating Policies

US SBU ACCESS MANAGEMENT POLICY

Policy Owner: US SBU Information Technology - Governance

Original issue Date: 05/29/2015

Revision Date: n/a

US SBU ACCESS MANAGEMENT POLICY

Contents

| | | |
|--------------|---|----------|
| 1.0 | Introduction..... | 1 |
| 2.0 | Scope..... | 1 |
| 3.0 | Definitions..... | 1 |
| 3.1 | End User..... | 1 |
| 3.2 | Access Provisioning..... | 1 |
| 3.3 | Privileged IT Access..... | 1 |
| 3.4 | Privileged IT Account Characteristics..... | 1 |
| 3.4.1 | Administrator..... | 1 |
| 3.4.2 | Individual..... | 1 |
| 3.4.3 | Shared..... | 2 |
| 3.4.4 | System Delivered/Default..... | 2 |
| 3.4.5 | Service..... | 2 |
| 4.0 | Access Management Policy..... | 3 |
| 4.1 | Authentication..... | 3 |
| 4.2 | Account Provisioning..... | 3 |
| 4.3 | Segregation of Duties..... | 3 |
| 4.4 | Periodic Access Review..... | 3 |
| 5.0 | APPROVALS..... | 4 |
| 6.0 | Version Control History..... | 5 |

| |
|---|
| Document Control No.: IT-005 Last Revised Date: 5-22-2015 Page 1 |
|---|

US SBU ACCESS MANAGEMENT POLICY

1.0 *Introduction*

This policy addresses topics specific to segregation of duties, access provisioning, monitoring use of, and access to AES US critical applications and related infrastructure (system/database).

2.0 *Scope*

This policy is applicable to AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, and any affiliate of US Services that adopts this policy pursuant to its own corporate governance procedures (collectively, the "Companies"). Documentation of adoption of this policy by a US Services affiliate shall be kept by the US Services Policy Committee or its designate. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp.

3.0 *Definitions*

3.1 *End User*

Individuals with authorized access to US SBU technology resources including permanent and temporary employees or third party personnel such as temporaries, contractors, consultants, and other parties provisioned interactive access to individual accounts within the AES US business systems

3.2 *Access Provisioning*

Access Provisioning is defined as the act of creating, modifying, or deleting user accounts to allow access to a system or application, or to alter the rights allowed by that account

3.3 *Privileged IT Access*

Privileged access allows the management of logical access, change management, daily operations management and monitoring

3.4 *Privileged IT Account Characteristics*

(Accounts can have multiple characteristics)

3.4.1 *Administrator*

Any interactive user account with Admin rights as defined by the OS/Database/Application

3.4.2 *Individual*

Any interactive user account to which only one individual user is authorized to use the account. Also describes a non-privileged (end-user) account type

| |
|---|
| Document Control No.: IT-005 Last Revised Date: 5-22-2015 Page 2 |
|---|

US SBU ACCESS MANAGEMENT POLICY

3.4.3 Shared

Any interactive user account for which more than one individual user is authorized to use the account

3.4.4 System Delivered/Default

Any generic system account created by the OS/Database/Application upon its installation. The account can be utilized by the system and/or an authorized interactive user

3.4.5 Service

Any account that a service uses to perform its designated function. This account can be utilized by the system and/or an authorized interactive user

| |
|---|
| Document Control No.: IT-005 Last Revised Date: 5-22-2015 Page 3 |
|---|

US SBU ACCESS MANAGEMENT POLICY

4.0 Access Management Policy

4.1 Authentication

AES US critical systems/applications must require authentication sufficient to secure and identify the use of an account.

4.2 Account Provisioning

For AES US systems/applications, the Access Provisioning Processes requires appropriate management approval which must be documented and retained.

ALL access permissions must be appropriately authorized and maintained on the basis of Least Privilege. This includes when an account is created, or a user's role changes, i.e. transfer or termination.

4.3 Segregation of Duties

Segregation of duties must be maintained over requesting, approving, granting, and monitoring access to all accounts.

4.4 Periodic Access Review

Access rights to ALL accounts of the AES US business systems must be reviewed periodically by management to validate appropriateness of access for job functions (on the basis of Least Privilege) following defined AES US User Access Management Processes.

Document Control No.: **IT-005**
Last Revised Date: **5-22-2015**
Page 4

US SBU ACCESS MANAGEMENT POLICY

5.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:

| | |
|--|----------------|
|  Mike Collier – US SBU IT Director | 7/1/15 Date |
|--|----------------|

Document Control No.: **IT-005**
Last Revised Date: 5-22-2015
Page 5

US SBU ACCESS MANAGEMENT POLICY

6.0 Version Control History

| <i>Date</i> | <i>Description of Changes</i> | <i>Author(s)</i> | <i>Approver(s)</i> |
|---------------------|--------------------------------|---------------------------------------|--------------------|
| <i>May 22, 2015</i> | <i>Initial Policy creation</i> | <i>IT Governance Mike Gardner</i> | |
| | | | |
| | | | |



AES US Strategic Business Unit (“US SBU”)

Information Technology Operating Policies

US SBU END-USER HARDWARE/SOFTWARE POLICY

Policy Owner: US SBU Information Technology - CIO

Original issue Date: 10/2/15

Revision Date: n/a

US SBU END-USER HARDWARE/SOFTWARE POLICY

Contents

| | | |
|-------|---|---|
| 1.0 | Introduction..... | 1 |
| 2.0 | Scope | 1 |
| 3.0 | Definitions | 1 |
| 3.1 | Standard Hardware and Software..... | 1 |
| 3.2 | Non-Standard Hardware and Software..... | 1 |
| 4.0 | Policy | 2 |
| 4.1 | Policy Objective | 2 |
| 4.2 | Standard Hardware/Software | 2 |
| 4.2.1 | Procurement..... | 2 |
| 4.2.2 | Configuration..... | 2 |
| 4.2.3 | Applications..... | 2 |
| 4.2.4 | Support | 2 |
| 4.3 | Non-Standard Hardware/Software | 3 |
| 4.3.1 | Procurement..... | 3 |
| 4.4 | Hardware Inventory | 3 |
| 4.5 | Software Licensing..... | 3 |
| 4.6 | Policy Exclusion..... | 3 |
| 4.7 | Enforcement | 3 |
| 5.0 | APPROVALS..... | 4 |
| 6.0 | Version Control History..... | 5 |

| |
|---|
| Document Control No.: JT-006 Last Revised Date: 10-02-2015 Page 1 |
|---|

US SBU END-USER HARDWARE/SOFTWARE POLICY

1.0 *Introduction*

AES US has established the following policy for the procurement, operation and support of End-user device hardware and software.

2.0 *Scope*

This policy is applicable to AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, and any affiliate of US Services that adopts this policy pursuant to its own corporate governance procedures (collectively, the "Companies"). Documentation of adoption of this policy by a US Services affiliate shall be kept by the US Services Policy Committee or it's designate. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp.

3.0 *Definitions*

3.1 *Standard Hardware and Software*

Equipment and Applications that are placed into the approved list for use, and will be an item normally supported by the AES US IT Support staff

3.2 *Non-Standard Hardware and Software*

Equipment and Applications that are not on the approved list, but are uniquely required for functional or other business reasons, support will be on a "Best Effort" basis, and may be a pass through to the vendor support team

US SBU END-USER HARDWARE/SOFTWARE POLICY

4.0 Policy

AES US has established the following policy for the procurement, allocation, operation and support of end-user devices and applications/software, including, but not limited to:

- Desktop computers
- Laptop computers
- Monitors
- Tablets
- Smartphones/Cell Phones
- WiFi Hotspots/Jetpacks
- Printers
- Telepresence/Video conferencing units
- Remote Access Tokens

4.1 Policy Objective

- *To establish AES US SBU IT responsibility to create standards, and to make sure those standards are supportable*
- *To establish AES US SBU IT responsibility to manage and support installed resources including maintenance and tracking of inventory and licenses*
- *To establish AES US SBU IT responsibility to provide for replacement of end of lifecycle equipment and software*
- *To collaborate with AES US SBU and Corporate Security teams to ensure company assets are protected*

4.2 Standard Hardware/Software

4.2.1 Procurement

All standard End-user device hardware and software will be procured by AES US IT in accordance with Procurement Policies and Procedures.

4.2.2 Configuration

Standard hardware configurations will be determined by AES US SBU IT, and updated as technology changes.

4.2.3 Applications

Standard software applications will be determined by AES US SBU IT, and updated as technology changes.

4.2.4 Support

AES US SBU IT provides support for all standard hardware and software.

| |
|--|
| Document Control No.: IT-006 Last Revised Date: 10-02-2015 Page 3 |
|--|

US SBU END-USER HARDWARE/SOFTWARE POLICY

4.3 Non-Standard Hardware/Software

4.3.1 Procurement

All non-standard End-user device hardware and software will be procured by AES US SBU IT in accordance with the AES US SBU Procurement Policies and Procedures, and with the approval of the appropriate AES US SBU IT authority.

AES US SBU IT will provide a mechanism to receive requests for evaluation of non-standard Hardware/Software.

4.4 Hardware Inventory

AES US SBU IT is solely responsible for adding, removing or changing the location of any AES US SBU hardware (desktop computers, laptop assignees, printers, etc.).

Lost or Stolen equipment must be reported to AES US SBU IT immediately.

All company equipment shall be returned to AES US SBU IT upon an employee or contractor termination.

4.5 Software Licensing

AES US SBU employees are required to adhere to copyrights and terms of all software licenses to which AES is a party.

Only Company-licensed software may be installed on Company-owned hardware, unauthorized software may be removed without notice.

4.6 Policy Exclusion

Any exclusion(s) to this policy must be approved by the CIO.

4.7 Enforcement

Failure to comply with this policy may result in disciplinary action.

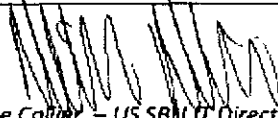
Document Control No.: **IT-006**
Last Revised Date: **10-02-2015**
Page 4

US SBU END-USER HARDWARE/SOFTWARE POLICY

5.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:

| | |
|--|---|
|  Mike Collier – US SBU IT Director |  Date |
|--|---|

Document Control No.: **IT-006**
Last Revised Date: **10-02-2015**
Page 5

US SBU END-USER HARDWARE/SOFTWARE POLICY

6.0 Version Control History

| Date | Description of Changes | Author(s) | Approver(s) |
|--------------|-------------------------|-------------------------------|-------------|
| Oct. 2, 2015 | Initial Policy creation | IT Governance Mike Gardner | |
| | | | |
| | | | |



AES US Strategic Business Unit ("US SBU")

Information Technology Operating Policies

US SBU IT ACCEPTABLE USE POLICY

Policy Owner: US SBU Information Technology - CIO

Original issue Date: 10/02/2015

Revision Date: n/a

US SBU IT ACCEPTABLE USE POLICY

Contents

| | | |
|-----|------------------------------|---|
| 1.0 | Introduction..... | 1 |
| 2.0 | Scope | 1 |
| 3.0 | Definitions | 1 |
| 3.1 | IT Resource | 1 |
| 3.2 | Personal Information..... | 1 |
| 4.0 | Policy | 2 |
| 4.1 | General Restrictions | 2 |
| 4.2 | Computer Systems..... | 2 |
| 4.3 | E-Mail | 2 |
| 4.4 | Internet Access | 3 |
| 4.5 | Instant Messaging | 3 |
| 4.6 | Text Messaging | 3 |
| 4.7 | Printing..... | 4 |
| 4.8 | Voice..... | 4 |
| 4.9 | Enforcement | 4 |
| 5.0 | APPROVALS..... | 5 |
| 6.0 | Version Control History..... | 6 |

| |
|--|
| Document Control No.: IT-007 Last Revised Date: 10-02-2015 Page 1 |
|--|

US SBU IT ACCEPTABLE USE POLICY

1.0 *Introduction*

The purpose of this policy is to outline the acceptable use of IT provided resources and equipment at AES US. These rules are in place to protect the employee and AES US. Inappropriate use exposes AES US to risks including virus attacks, compromise of network systems and services, and legal issues.

2.0 *Scope*

This policy is applicable to AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, and any affiliate of US Services that adopts this policy pursuant to its own corporate governance procedures (collectively, the "Companies"). Documentation of adoption of this policy by a US Services affiliate shall be kept by the US Services Policy Committee or its designate. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp.

3.0 *Definitions*

3.1 *IT Resource*

Any service or component provided or maintained by IT.

3.2 *Personal Information*

For the purpose of this document we are using the definition of Personally Identifiable Information from <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>:

PII is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

US SBU IT ACCEPTABLE USE POLICY

4.0 ***Policy***

4.1 ***General Restrictions***

Users will adhere to the following restrictions for use of all Assets provided by IT; more specific restrictions are listed by type of resource.

- At All times, AES People and contractors have the responsibility to use all provided services in a responsible, professional, ethical, and lawful manner
- Copyright laws, ethics rules, and other applicable laws are to be abided by
- Company Resources, including information, must be protected
- All access to Company resources must adhere to the Access Management Policy
- Use only accounts assigned to you, and only for their intended business purpose
- Do not share your accounts/passwords with anyone
- Do not attempt to hack any company systems or accounts
- Protective systems installed by IT or Security (e.g. Anti-virus, DLP, Intrusion prevention/protection systems, and Malware protection) must not be disabled or bypassed
- Company resources are to be used for Business only, not for personal gain
- All information stored, sent, or received on AES US systems is the property of AES
- AES US IT reserves the right to monitor usage of all systems and services including information stored in or transmitted between systems without notice
- Material that is abusive, threatening, fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful, is not acceptable to store or transmit on any company resources
- Messages that disclose personal information without authorization are prohibited
- Electronic communications, including e-mail, voice-mail, instant messaging, text messaging, or faxes, should never be considered private or secure

4.2 ***Computer Systems***

- Only company-owned systems may be connected to the corporate network without a Security review
- Access to unattended systems must be prevented (i.e. logged off, or locked)
- Unauthorized software installation is prohibited

4.3 ***E-Mail***

At all times, AES people and contractors have the responsibility to use the e-mail system, as well as other computer resources, in a responsible, professional, ethical, and lawful manner.

- Employee use of accounts not assigned by US SBU for business communications is prohibited
- E-mail could be stored indefinitely on other computers, including that of the recipient, do not assume deleting it from your system has eliminated all copies

US SBU IT ACCEPTABLE USE POLICY

- E-mail communications sent or received by an employee may be disclosed to law enforcement officials without notice
- Forging of e-mail header information or identity spoofing is prohibited

4.4 *Internet Access*

AES US provides Internet access to network users as needed to aid in facilitating and conducting Company business.

- Assume all information retrieved from the Internet is copyrighted information
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AES US does not have an active license is strictly prohibited
- Assume anything posted to the Internet cannot be erased

4.5 *Instant Messaging*

AES US provides instant messaging capability to network users to aid and facilitate business communications internally with other AES employees. Instant messaging to external accounts is permitted only for business purposes.

Unacceptable Instant Messaging use – the following activities are, in general prohibited. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable use.

- Instant messaging for non-business purposes
- Using instant messaging to interfere with the ability of others to conduct AES business
- Using instant messaging for any purpose which violates State or Federal law, or AES policy

4.6 *Text Messaging*

At all times, AES people and contractors have the responsibility to use text messaging, as well as other computer resources, in a responsible, professional, ethical, and lawful manner.

Unacceptable text messaging use – the following activities are, in general prohibited. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable use.

- Using text messages to interfere with the ability of others to conduct AES business
- Using text messages for any purpose which violates State or Federal law, or AES policy

US SBU IT ACCEPTABLE USE POLICY

4.7 Printing

At all times, AES people and contractors have the responsibility to use the printing systems, as well as other computer resources, in a responsible, professional, ethical, and lawful manner.

Unacceptable printing system use – the following activities are, in general prohibited. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable use.

- Using the printing system to interfere with the ability of others to conduct AES business
- Printing and leaving confidential information unattended at the printer
- Using the printing system for any purpose which violates State or Federal law, or AES policy

4.8 Voice

At all times, AES people and contractors have the responsibility to use the Phone and Voice-Mail systems, as well as other computer resources, in a responsible, professional, ethical, and lawful manner.

- Voice-mail could be stored indefinitely on other devices, including that of the recipient, do not assume deleting it from your device has eliminated all copies
- Copyright laws, ethics rules, and other applicable laws are to be abided by

4.9 Enforcement

Failure to comply with this policy may result in disciplinary action.

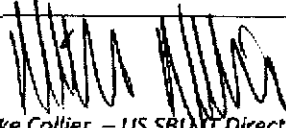
Document Control No : **IT-007**
Last Revised Date: **10-02-2015**
Page 5

US SBU IT ACCEPTABLE USE POLICY

5.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:



| | |
|--|-----------------|
|  Mike Collier – US SBU IT Director | 10/5/15 Date |
|--|-----------------|

Document Control No. IT-007
Last Revised Date: 10-02-2015
Page 6

US SBU IT ACCEPTABLE USE POLICY

6.0 Version Control History

| Date | Description of Changes | Author(s) | Approver(s) |
|--------------|-------------------------|-------------------------------|-------------|
| Oct 02, 2015 | Initial Policy creation | IT Governance Mike Gardner | |
| | | | |
| | | | |

| | | |
|--|--|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-010-000 IT SECURITY POLICY | Original Issue Date: <u>11/16/2007</u> |
| | | Revision Number: <u>9.04</u> |
| | | Last Revision: <u>4/9/2012</u> |

REFERENCES

| | | | | | | | | |
|---|--|--|--|--|--|--|--|--|
| <input checked="" type="checkbox"/> Corporate | | | <u>SOP APPLICABILITY</u> <input type="checkbox"/> Business Unit | | | <input type="checkbox"/> Department | | |
| <input type="checkbox"/> Operational Procedure | | | <u>SOP TYPE</u> <input type="checkbox"/> Business Practice | | | <input checked="" type="checkbox"/> Policy Statement | | |
| <input type="checkbox"/> Confidential | | | <input checked="" type="checkbox"/> Business Sensitive/Limited Distribution | | | <input type="checkbox"/> Available for Public Distribution | | |
| <u>COMPLIANCE</u> [Check all that apply] | | | | | | | | |
| <input type="checkbox"/> FERC Code of Conduct | | | <input type="checkbox"/> PUCO Code of Conduct | | | | | |
| <input type="checkbox"/> NERC Reliability Standards | | | <input type="checkbox"/> PUCO CAM | | | | | |
| <input type="checkbox"/> NERC Compliance | | | <input type="checkbox"/> PUCO Reliability Compliance | | | | | |
| <input type="checkbox"/> NERC Data Confidentiality | | | <input checked="" type="checkbox"/> Other [please specify]: General Business Policy | | | | | |
| <input checked="" type="checkbox"/> SOX | | | <input type="checkbox"/> None | | | | | |

DESCRIPTION**1.0 Purpose**



- 1.1. This policy documents the overall IT Security Policy for DPL networked computer systems. Additional policies, procedures and standards document specific expectations.

2.0 Scope

- 2.1. This policy applies to all personnel accessing DPL computer resources.

3.0 Definitions

- 3.1. DPL – The operating divisions of both DPL Inc. and The Dayton Power & Light Company (DP&L).
- 3.2. Confidentiality – Refers to DPL's needs, obligations and desires to protect private, proprietary and other sensitive information from those who do not have the right and need to obtain it.
- 3.3. Access – Defines rights, privileges, and mechanisms to protect assets from access or loss.
- 3.4. Accountability – Defines the responsibilities of users, operations staff, and management.
- 3.5. Authentication – Establishes password and authentication policy.

| | | |
|--|--|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-010-000 IT SECURITY POLICY | Original Issue Date: <u>11/16/2007</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|--|--|---|

- 3.6. Availability – Establishes hours of resource availability, redundancy and recovery, and maintenance downtime periods.

4.0 Policy

4.1. Confidentiality

All customer and Company information is to be used exclusively for DPL business. Data must be kept accurate and not altered or falsified for personal gain or malicious intent. All Company data, including customer data, security information, computer information, organization charts, the Company phone book, and policies should not be disclosed to anyone without proper authority. Computer data must not be copied without having first obtained permission from the data owner.

Communications via the internet, including e-mail, is not confidential. While using Company networks, remember that you are a representative of the Company and all rules of responsible business etiquette apply. You should not expect privacy or confidential usage of DPL resources. Users may not alter or copy a file belonging to another network user without first obtaining permission from the owner of the file. The capability to access a file does not imply permission to read, alter, or copy that file. Monitoring or accessing another user's information may not be done without business reasons and authorization. Do not attempt to gain unauthorized access to resources or information. Do not attempt to bypass data protection measures, search for security loopholes, and alter software protections or restrictions placed on computer applications, files, or directories.

DPL reserves the right to examine computer records or monitor activities of individual users, for any reason at any time.

4.2. Access


No one may access confidential records unless specifically authorized to do so. Authorized individuals may use confidential records only for authorized purposes. DPL requires network users not to access or intercept files or data of others without permission, and not to use another's password or access files under false identity.

Technology assets are to be housed in an appropriately secure physical location. Laptops should not be left out overnight but locked in a secure location. Technology assets include servers, personal computers that house systems with controlled access, ports, sniffing devices, and network components (routers, switches, firewalls, etc).

Passwords restrict use of DPL systems and networks to authorized users. Each authorized user is assigned a unique password that is to be protected by that individual and not shared with others, strong, is changed on a regular basis, and is deleted when no longer authorized.

4.3. Privacy

All electronic documents, including but not limited to, any data created, stored, sent or received, and email, are Company records, and are Company property. The Company reserves the right to

| | | |
|---|--|---|
|  | DPL STANDARD OPERATING PROCEDURE POL-010-000 IT SECURITY POLICY | Original Issue Date: <u>11/16/2007</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|---|--|---|

audit, access, and disclose all active and/or archived documents for any purpose. Full cooperation is required during audits.

DPL computer resources contain standard system monitoring tools. These tools log events and activities. All logons, logoffs, program access and data manipulation, Internet sites visited, and e-mail sent and received can be scanned by automated tools and monitored by date, time, and user. Access to certain Internet sites may be blocked based on an industry rating system for sexual content, entertainment, shopping, and other non-productive content. Internet e-mails with oversized or executable file attachments may be blocked. Virus protection software scans e-mail and attachments for virus infected files. Questions should be directed to the IT Help Desk.

4.4. Accountability

Individual users are responsible for ensuring that others do not use their system privileges. In particular, users must take great care in protecting their usernames and passwords from eavesdropping or careless misplacement. Passwords are never to be "loaned". Individual users may be held responsible for security violations associated with their usernames.

Information Technology (IT) operations staff is responsible for reviewing audit logs and identifying potential security violations. The operations staff is responsible for establishing the security and access control mechanisms and may be held accountable for any security breaches that arise from improper configuration of these mechanisms. If the operations staff believes a security incident has occurred, they will immediately notify their management. IT management will assess the potential implications of the incident and take any remedial and necessary action.

Each user permitted to access a controlled system is to be made aware of this policy and the Acceptable Use Policy. Management will provide this information and training to the user within 90 days of network account activation.



Adding or removal of software to computers and networks must be authorized by DPL IT, system defaults reviewed for potential security hole, and default accounts and passwords must be changed.

Authentication and data encryption or point-to-point communication will be implemented for all systems that send or receive sensitive data or when it is critical that both parties know with whom they are communicating. The decision of whether to encrypt data should be made by the professional system administrator responsible for the particular application being distributed and IT Security, with the knowledge of the data owner.

- 4.5. Enforcement - Any employee found to have violated this policy, and supporting IT policies may be subject to disciplinary action, up to and including termination of employment.

5.0 Responsibilities

- 5.1. Infrastructure team and Application team are jointly responsible for the review, revision and implementation of this policy and its associated procedures.

| | | |
|--|--|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-010-000 IT SECURITY POLICY | Original Issue Date: <u>11/16/2007</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|--|--|---|

- 5.1.1. This policy shall be reviewed and updated at least every two (2) years, and updated as required.

ACKNOWLEDGEMENTS AND APPROVALS

The following have reviewed and approved this policy:

Originated/Revised by:

Apr 9 2012 4:52 PM

X

Dustin Bassler

Bassler, Dustin

Approved:

Apr 10 2012 8:02 AM

X

David Hoskins



Hoskins, David

Apr 19 2012 2:08 PM

X

Julie A. Pike

Pike, Juli

| | | |
|--|--|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-010-000 IT SECURITY POLICY | Original Issue Date: <u>11/16/2007</u> |
| | | Revision Number: <u>9.04</u> |
| | | Last Revision: <u>4/9/2012</u> |

Jun 6 2012 1:30 PM

X *Scott Kelly*
 Kelly, Scott



Revision History

| Revision Number | Date Revised | Approved By | Revision Description |
|-----------------|-------------------|-------------|--|
| <u>0</u> | <u>11/16/2007</u> | | <u>Original Document</u> |
| <u>9.01</u> | <u>8/26/2009</u> | | Signature block updated, Section 4.2 modified to include a rule for securing laptops and "difficult to crack" has been replaced with "strong." Section 4.6 "Availability" removed |
| <u>9.02</u> | <u>8/17/2010</u> | | Section 4.4 language updated surrounding training, addition or removal software and default accounts. Section 4.5 updated to include IT Security. Section 5.1 titles removed. Signature block update |
| <u>9.03</u> | <u>1/6/12</u> | | <u>Acknowledgements and approvals update. Changed review timeframe from "annually" to "every two (2) years."</u> |
| <u>9.04</u> | <u>4/9/12</u> | | <u>Updated 5.1 language, added CoSign signature blocks.</u> |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

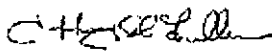
Annual Review:

5 of 6



DPL – Business Sensitive/Limited Distribution

| | | |
|--|--|---|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-010-000</p> <p align="center">IT SECURITY POLICY</p> | <p>Original Issue Date: <u>11/16/2007</u></p> <p>Revision Number: <u>9.04</u></p> <p>Last Revision: <u>4/9/2012</u></p> |
|--|--|---|

Jun 15 2012 2:38 PM

X 

Fuller, Jeffrey K.

| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-040-000 IT SECURITY TRAINING POLICY | Original Issue Date: <u>01/14/2008</u> |
| | | Revision Number: <u>9.03</u> |
| | | Last Revision: <u>4/9/2012</u> |

REFERENCES

| | | |
|---|---|--|
| <u>SOP APPLICABILITY</u> | | |
| <input checked="" type="checkbox"/> Corporate | <input type="checkbox"/> Business Unit | <input type="checkbox"/> Department |
| <u>SOP TYPE</u> | | |
| <input type="checkbox"/> Operational Procedure | <input type="checkbox"/> Business Practice | <input checked="" type="checkbox"/> Policy Statement |
| <u>SOP SENSITIVITY</u> | | |
| <input type="checkbox"/> Confidential | <input checked="" type="checkbox"/> Business Sensitive/Limited Distribution | <input type="checkbox"/> Available for Public Distribution |
| <u>COMPLIANCE</u> | | |
| [Check all that apply] | | |
| <input type="checkbox"/> FERC Code of Conduct | <input type="checkbox"/> PUCO Code of Conduct | |
| <input type="checkbox"/> NERC Reliability Standards | <input type="checkbox"/> PUCO CAM | |
| <input type="checkbox"/> NERC Compliance | <input type="checkbox"/> PUCO Reliability Compliance | |
| <input type="checkbox"/> NERC Data Confidentiality | <input checked="" type="checkbox"/> Other [please specify]: IT Policy | |
| <input type="checkbox"/> SOX | <input type="checkbox"/> None | |

DESCRIPTION**1.0 Purpose**

- 1.1. This policy ensures that computer users are trained annually on IT security policies and their computer responsibilities to protect DPL computer systems and information.

2.0 Scope



- 2.1. This policy applies to all personnel (employees, contractors, temporary employees and consultants) at DPL using computer systems or resources owned or leased.

3.0 Definitions

- 3.1. DPL – The operating divisions of both DPL Inc. and Dayton Power & Light Company (DP&L).

4.0 Policy



- 4.1. DPL shall provide information security awareness and training to all DPL employee computer users annually and to new DPL employee computer users within approximately 90 days of account activation.

| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-040-000 IT SECURITY TRAINING POLICY | Original Issue Date: <u>01/14/2008</u> Revision Number: <u>9.03</u> Last Revision: <u>4/9/2012</u> |
|--|---|---|

- 4.2. Information Technology (IT) shall ensure computer users are aware of the information security policies, procedures or guidelines and have access to current versions.
- 4.3. The information security awareness and training shall cover information security basics, computer user responsibilities, and all related IT Security policies with computer user responsibilities.
- 4.4. DPL employee computer users shall acknowledge that they have been trained and informed, and are aware of DPL Information Security policies, and their role in protecting DPL information systems and assets, by signing an acknowledgement form at the completion of training.
- 4.5. Area Managers and supervisors are responsible for reviewing the information security program with contractors, temporary employees and consultants who they have authorized for access to DPL computer resources.
 - 4.5.1. The information security training program shall be made available by IT to area managers and supervisors.
- 4.6. Documentation Maintenance – Documentation and evidence to support this policy shall be kept for 12 months.
- 4.7. Enforcement - Anyone found to have violated these policies may be subject to computer account being disabled, disciplinary action, up to and including termination of employment or contract for contractors, consultants or other entities.

5.0 Responsibilities

- 5.1. The CIO is responsible for the review, revision and implementation of this policy
 - 5.1.1. This policy shall be reviewed and updated at least annually, and updated as required.

| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-040-000 IT SECURITY TRAINING POLICY | Original Issue Date: <u>01/14/2008</u> Revision Number: <u>9.03</u> Last Revision: <u>4/9/2012</u> |
|--|---|---|

ACKNOWLEDGEMENTS AND APPROVALS

The following have reviewed and approved this policy:

Originated/Revised by:

Apr 12 2012 4:32 PM

X

Dustin Bassler

Bassler, Dustin

Approved:

Apr 16 2012 11:47 AM

X

David Hoskins

Hoskins, David

Jul 23 2012 12:00 PM



X

Scott Kelly



Kelly, Scott

Revision History

| Revision Number | Date Revised | Approved By | Revision Description |
|-----------------|------------------|-------------|--------------------------------|
| <u>0</u> | <u>1/14/2008</u> | | <u>Original document</u> |
| <u>9.01</u> | <u>8/26/2009</u> | | <u>Signature block updated</u> |


| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-040-000 IT SECURITY TRAINING POLICY | Original Issue Date: <u>01/14/2008</u> |
| | | Revision Number: <u>9.03</u> |
| | Last Revision: <u>4/9/2012</u> | |

| | | | |
|-------------|-------------------|--|--|
| <u>9.02</u> | <u>11/21/2011</u> | | <u>Acknowledgements and approvals updated.</u> |
| <u>9.03</u> | <u>4/9/2012</u> | | <u>Added CoSign signature blocks.</u> |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |



| | | |
|--|---|---|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-040-000</p> <p align="center">IT SECURITY TRAINING POLICY</p> | <p>Original Issue Date: <u>01/14/2008</u></p> <p>Revision Number: <u>9.03</u></p> <p>Last Revision: <u>4/9/2012</u></p> |
|--|---|---|

Annual Review:

Jul 26 2012 11:02 AM

X 

Fuller, Jeffrey K.

| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-090-000 SECURITY INCIDENT MANAGEMENT POLICY | Original Issue Date: <u>04/20/2008</u> |
| | | Revision Number: <u>9.04</u> |
| | | Last Revision: <u>4/11/2012</u> |

REFERENCES

| | | |
|--|---|--|
| <u>SOP APPLICABILITY</u> <input type="checkbox"/> Corporate <input type="checkbox"/> Business Unit <input checked="" type="checkbox"/> Department | | |
| <u>SOP TYPE</u> <input type="checkbox"/> Operational Procedure <input type="checkbox"/> Business Practice <input checked="" type="checkbox"/> Policy Statement | | |
| <u>SOP SENSITIVITY</u> <input type="checkbox"/> Confidential <input checked="" type="checkbox"/> Business Sensitive/Limited Distribution <input type="checkbox"/> Available for Public Distribution | | |
| <u>COMPLIANCE</u> [Check all that apply] | | |
| <input type="checkbox"/> FERC Code of Conduct <input type="checkbox"/> NERC Reliability Standards <input type="checkbox"/> NERC Compliance <input type="checkbox"/> NERC Data Confidentiality <input type="checkbox"/> SOX | <input type="checkbox"/> PUCO Code of Conduct <input type="checkbox"/> PUCO CAM <input type="checkbox"/> PUCO Reliability Compliance <input checked="" type="checkbox"/> Other [please specify]: <u>IT Business Policy</u> <input type="checkbox"/> None | |

DESCRIPTION**1.0 Purpose**



- 1.1. This policy ensures that a plan is in place to identify, respond, classify, and communicate security incidents related to DPL Inc. domain computing resources.

2.0 Scope

- 2.1. This policy applies to personnel responsible for management and support of the DPL network infrastructure and applications.

3.0 Definitions

- 3.1. DPL – The operating divisions of both DPL Inc. and Dayton Power & Light Company (DP&L).
 3.2. DPL Security – Department within Dayton Power & Light Company that encompasses physical security, safety, and facilities.
 3.3. Security Incident - Any act or suspicious event that compromises, or was an attempt to compromise, the electronic security perimeter or physical security perimeter of a DPL asset, or, disrupts, or was an attempt to disrupt, the operation of a DPL computing resources.



| | | |
|--|---|--|
|   | DPL STANDARD OPERATING PROCEDURE POL-090-000 SECURITY INCIDENT MANAGEMENT POLICY | Original Issue Date: <u>04/20/2008</u> Revision Number: <u>9.04</u> Last Revision: <u>4/11/2012</u> |
|--|---|--|

4.0 Policy

- 4.1. A security management procedure shall be documented and maintained. (Ref: Security Incident Response Procedure PROC-090-001).
- 4.2. The incident response procedure shall include:
 - 4.2.1. Roles and responsibilities of incident response team members
 - 4.2.2. Incident handling procedures
 - 4.2.3. Communication/Reporting plans
- 4.3. The security incident response procedure shall include the characterization and classification of events as reportable incidents.
- 4.4. Security incidents shall be documented by IT security, and reported to senior IT management.
- 4.5. If no reportable security incidents occur, the security incident response procedure shall be tested annually.
- 4.6. Documentation relating to a reportable security incident, or testing, shall be retained for 2 years.
- 4.7. Enforcement - Any employee found to have violated these policies may be subject to disciplinary action, up to and including termination of employment.

5.0 Responsibilities

- 5.1. The Chief Information Officer (CIO) is responsible for the review, revision and implementation of this policy and its associated procedures.
 - 5.1.1. This policy shall be reviewed and updated at least annually, and updated as required.

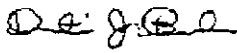
| | | |
|--|---|--|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-090-000</p> <p align="center">SECURITY INCIDENT MANAGEMENT POLICY</p> | <p>Original Issue Date: <u>04/20/2008</u></p> <p>Revision Number: <u>9.04</u></p> <p>Last Revision: <u>4/11/2012</u></p> |
|--|---|--|

ACKNOWLEDGEMENTS AND APPROVALS

The following have reviewed and approved this policy:


Originated/Revised by:

Apr 12 2012 4:33 PM

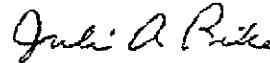
X 
 Bassler, Dustin

Approved:

Apr 16 2012 11:49 AM



X 
 Hoskins, David

Apr 26 2012 7:38 AM



X 
 Rike, Juli

Revision History

| Revision Number | Date Revised | Approved By | Revision Description |
|-----------------|----------------|-------------|---------------------------|
| <u>0</u> | <u>4/20/08</u> | | <u>Original Document.</u> |

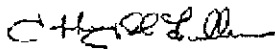
| | | |
|--|---|--|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-090-000</p> <p align="center">SECURITY INCIDENT MANAGEMENT POLICY</p> | <p>Original Issue Date: <u>04/20/2008</u></p> <p>Revision Number: <u>9.04</u></p> <p>Last Revision: <u>4/11/2012</u></p> |
|--|---|--|

| | | | |
|-------------|------------------|--|---|
| <u>9.01</u> | <u>8/26/2009</u> | | <u>Update to signature blocks, update Director of IT to Vice President and CIO within document.</u> |
| <u>9.02</u> | <u>7/27/10</u> | | <u>Update to section 1.1. Specified DPL Inc. Domain and removed "including Energy Management."</u> |
| <u>9.03</u> | <u>1/9/2012</u> | | <u>Updated Acknowledgements and Approvals.</u> |
| <u>9.04</u> | <u>4/12/2012</u> | | <u>Added CoSign signature blocks.</u> |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |



| | | |
|--|---|--|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-090-000</p> <p align="center">SECURITY INCIDENT MANAGEMENT POLICY</p> | <p>Original Issue Date: <u>04/20/2008</u></p> <p>Revision Number: <u>9.04</u></p> <p>Last Revision: <u>4/11/2012</u></p> |
|--|---|--|

Annual Review:

Jun 12 2012 10:05 AM

X 

Fuller, Jeffrey K.

| | | |
|--|--|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-140-000 REMOTE ACCESS POLICY | Original Issue Date: <u>01/20/2008</u> |
| | | Revision Number: <u>9.04</u> |
| | | Last Revision: <u>4/9/2012</u> |

REFERENCES

| | | |
|---|---|--|
| <u>SOP APPLICABILITY</u> | | |
| <input checked="" type="checkbox"/> Corporate | <input type="checkbox"/> Business Unit | <input type="checkbox"/> Department |
| <u>SOP TYPE</u> | | |
| <input type="checkbox"/> Operational Procedure | <input type="checkbox"/> Business Practice | <input checked="" type="checkbox"/> Policy Statement |
| <u>SOP SENSITIVITY</u> | | |
| <input type="checkbox"/> Confidential | <input checked="" type="checkbox"/> Business Sensitive/Limited Distribution | <input type="checkbox"/> Available for Public Distribution |
| <u>COMPLIANCE</u> | | |
| [Check all that apply] | | |
| <input type="checkbox"/> FERC Code of Conduct | <input type="checkbox"/> PUCO Code of Conduct | |
| <input type="checkbox"/> NERC Reliability Standards | <input type="checkbox"/> PUCO CAM | |
| <input type="checkbox"/> NERC Compliance | <input type="checkbox"/> PUCO Reliability Compliance | |
| <input type="checkbox"/> NERC Data Confidentiality | <input checked="" type="checkbox"/> Other [please specify]: IT Business Policy | |
| <input type="checkbox"/> SOX | <input type="checkbox"/> None | |

DESCRIPTION**1.0 Purpose**



- 1.1. This policy outlines controls for connecting to the DPL network from any remote host, to minimize the potential exposure to DPL from damages which may result from unauthorized use of DPL resources.

2.0 Scope

- 2.1. This policy applies to all authorized DPL employees, contractors, vendors and agents with a DPL-owned or personally-owned computer used to connect to the DPL network remotely to do work on behalf of DPL.
- 2.2. Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, cable modem, DSL, SSL, Terminal Services, and VPN.

3.0 Definitions



- 3.1. DPL – The operating divisions of both DPL Inc. and Dayton Power & Light Company (DP&L).

| | | |
|--|--|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-140-000 REMOTE ACCESS POLICY | Original Issue Date: <u>01/20/2008</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|--|--|---|

- 3.2. Cable Modem - Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
- 3.3. Dial-in Modem - A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
- 3.4. Dual Homing - Having concurrent connectivity to more than one network from a computer or network device. (Examples: A - Remotely connected to the DPL Corporate network by a local Ethernet connection, and dialing into AOL or other Internet service provider, or any other remote network such as a spouse's work remote access. B- Configuring an ISDN router to dial into DPL and an ISP, depending on packet destination).
- 3.5. DSL - Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
- 3.6. Remote Access - Any access to DPL's corporate network through a non-DPL controlled network, device, or medium.
- 3.7. Split-tunneling - Simultaneous direct access to a non-DPL network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into DPL's corporate network via a VPN tunnel.
- 3.8. SSH - A network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer.
- 3.9. Virtual Private Network (VPN) - A method for accessing a remote network via "tunneling" through the Internet.

4.0 Policy

- 4.1. It is the responsibility of each authorized remote user, to ensure their remote access connection is given the same consideration as the user's on-site connection to the DPL network.
- 4.2. Adherence to all Corporate and Information Technology (IT) policies, computer usage and security protection apply when connected to the DPL network, regardless if you are working remotely or on-site.
- 4.3. Remote access connections to the DPL network are subject to monitoring.
- 4.4. Remote access needs to be authorized by a user's area manager, and the Network Service Manager in IT. IT will maintain an access control listing of personnel with remote access.
- 4.5. Secure remote access will be controlled using the following authentication methods: one-time password (SecureID Token), private key, certificates, RADIUS, or a combination of these methods.

| | | |
|--|--|---|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-140-000</p> <p align="center">REMOTE ACCESS POLICY</p> | <p>Original Issue Date: <u>01/20/2008</u></p> <p>Revision Number: <u>9.04</u></p> <p>Last Revision: <u>4/9/2012</u></p> |
|--|--|---|



- 4.6. Configuration of DPL owned equipment for split-tunneling or dual-homing is forbidden. User's home equipment that is configured for split-tunneling or dual-homing may not be used for the purpose of attaching to the DPL network.
- 4.7. Software and certificates required for remote access VPN into the DPL corporate network shall only be installed on DPL owned equipment, by the Information Technology department.
- 4.8. Remote access to external facing devices shall be protected and forbidden.

5.0 Enforcement

- 5.1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Responsibilities

- 6.1. The Infrastructure team is responsible for the review, revision and implementation of this policy and its associated procedures.
 - 6.1.1. This policy shall be reviewed and updated at least every two (2) years, and updated as required.

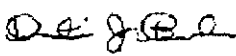
| | | |
|--|--|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-140-000 REMOTE ACCESS POLICY | Original Issue Date: <u>01/20/2008</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|--|--|---|

ACKNOWLEDGEMENTS AND APPROVALS

The following have reviewed and approved this policy:

Originated/Revised by:

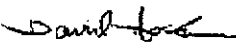
May 14 2012 4:26 PM

X 

Bassier, Dustin

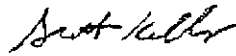
Approved:

Apr 24 2012 4:12 PM

X 

Hoskins, David



Jul 23 2012 11:55 AM

X 



Kelly, Scott

Revision History

| Revision Number | Date Revised | Approved By | Revision Description |
|-----------------|------------------|-------------|---|
| <u>0</u> | <u>1/20/2008</u> | | <u>Original document.</u> |
| <u>9.01</u> | <u>8/26/2009</u> | | Removed #4.6- Repeated in 4.7, Updated Signature Block. |

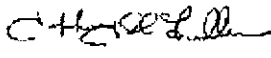
| | | |
|--|--|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-140-000 REMOTE ACCESS POLICY | Original Issue Date: <u>01/20/2008</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|--|--|---|

| | | | |
|-------------|------------------|--|--|
| <u>9.02</u> | <u>8/10/2010</u> | | Remove Section 4.8; reference to third party access procedure removed. |
| <u>9.03</u> | <u>1/6/2012</u> | | <u>Acknowledgements and approvals updated. Review timeline changed from "annually" to "every two (2) years."</u> |
| <u>9.04</u> | <u>4/9/2012</u> | | <u>Updated 6.1 language, added CoSign signature blocks.</u> |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |



| | | |
|--|--|---|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-140-000</p> <p align="center">REMOTE ACCESS POLICY</p> | <p>Original Issue Date: <u>01/20/2008</u></p> <p>Revision Number: <u>9.04</u></p> <p>Last Revision: <u>4/9/2012</u></p> |
|--|--|---|

Annual Review:

Jul 26 2012 11:04 AM

X 

Fuller, Jeffrey K.

| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-151-000 ANTI-VIRUS POLICY | Original Issue Date: <u>01/18/2008</u> |
| | | Revision Number: <u>9.04</u> |
| | | Last Revision: <u>4/9/2012</u> |

REFERENCES

| | | |
|---|--|--|
| <input checked="" type="checkbox"/> Corporate <input type="checkbox"/> Business Unit <input type="checkbox"/> Department | | |
| <u>SOP TYPE</u> <input type="checkbox"/> Operational Procedure <input type="checkbox"/> Business Practice <input checked="" type="checkbox"/> Policy Statement | | |
| <u>SOP SENSITIVITY</u> <input type="checkbox"/> Confidential <input checked="" type="checkbox"/> Business Sensitive/Limited Distribution <input type="checkbox"/> Available for Public Distribution | | |
| <u>COMPLIANCE</u> [Check all that apply] | | |
| <input type="checkbox"/> FERC Code of Conduct <input type="checkbox"/> NERC Reliability Standards <input type="checkbox"/> NERC Compliance <input type="checkbox"/> NERC Data Confidentiality <input checked="" type="checkbox"/> SOX | <input type="checkbox"/> PUCO Code of Conduct <input type="checkbox"/> PUCO CAM <input type="checkbox"/> PUCO Reliability Compliance <input checked="" type="checkbox"/> Other [please specify]: IT Business Policy <input type="checkbox"/> None | |

DESCRIPTION**1.0 Purpose**



- 1.1. This policy ensures that DPL assets are protected from malicious software, malware and viruses which can cause harm or destroy the integrity of DPL computer systems. The policy requires anti-virus and malware software prevention tools are used, where technically feasible, to protect Company systems.

2.0 Scope

- 2.1. This policy applies to all users and personnel responsible for management and support of DPL computer resources.

3.0 Definitions



- 3.1. DPL – The operating divisions of both DPL Inc. and Dayton Power & Light Company (DP&L).
- 3.2. Malware – Short for malicious software. Includes all computer viruses, worms, Trojan horses, or other similar programs that have the potential of damaging files stored on the computer system, affecting the performance of any application, or degrading the overall performance of DPL's computer network.

| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-151-000 ANTI-VIRUS POLICY | Original Issue Date: <u>01/18/2008</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|--|---|---|

- 3.3. Trojan Horse – A type of destructive malware that arrives as part of an email attachment and which otherwise appears harmless. However, it can affect the operation of the computer on which it is activated. Trojan horses do not typically infect other computers or spread from one computer to another.
- 3.4. User – Anyone with authorized access to DPL's computer resources including permanent and temporary employees or third party personnel such as temporaries, contractors, consultants, and other parties with valid DPL access accounts.
- 3.5. Virus and email virus – Pieces of code that "piggyback" on other programs and files that are transferred between computers by way of downloads, email or other types of file transfers. Each time the program is executed; the file is activated and can replicate itself and create havoc on the network by using up computing resources. Email viruses often replicate themselves automatically and can infect an email address book, sending itself out to dozens or even hundreds of other email users.
- 3.6. Worm – A piece of code that scans computer networks looking for specific flaws (or "holes") in other machines on the network, to which it replicates itself. Once there, it can perform malicious actions on the network, such as consuming large portions of computer resources or, in some cases, shutting down the network.

4.0 Policy



- 4.1. Protection against computer viruses, worms, Trojan horses, and other forms of malware is a vital aspect of computer network security. To keep computer systems running at optimum efficiency and free from malicious or infectious code that can create havoc on computer systems, current anti-virus software must be installed on all Windows based operating systems.
- 4.2. Users and Information Technology (IT) are responsible for ensuring that anti-virus software is installed and enabled on computers utilized to connect to the DPL network.
- 4.3. Users are forbidden from removing, disabling, stopping, and /or shutting down anti-virus software services and processes on a DPL computer.
- 4.4. Any activities with the intention to create and / or distribute malware, viruses, Trojan Horses, or worms on or from the DPL network and computing resources are forbidden. Network and computer activities may be monitored and logged to ensure compliance with this policy, and other Information Technology security policies and procedures.
- 4.5. Cases where anti-virus can not be installed, or configured for real-time monitoring must be documented on an anti-virus exception form noting compensating controls and acceptance of risk, and approved by the Enterprise Infrastructure Leadership.
- 4.6. Weekly scheduled scans are performed against WINDOWS servers on the DPL network.
- 4.7. Anti-virus real-time scans shall be configured to notify IT personnel of detected virus which can not be cured, and are renamed. Upon receipt, IT shall take prompt corrective action to eliminate the possible threat, including remove the infected machine from the DPL network.

| | | |
|--|---|---|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-151-000</p> <p align="center">ANTI-VIRUS POLICY</p> | <p>Original Issue Date: <u>01/18/2008</u></p> <hr/> <p>Revision Number: <u>9.04</u></p> <hr/> <p>Last Revision: <u>4/9/2012</u></p> |
|--|---|---|

- 4.8. Scheduled and real-time scan configuration settings shall be maintained and documented in the anti-virus procedures.
- 4.9. Anti-virus engine and signature updates shall be applied at least weekly to all Windows based operating systems (servers, desktops and laptops).
- 4.10. Documentation of scheduled scans shall be maintained for a minimum of 12 months. Anti-virus exception forms shall be maintained and reviewed annually for compliance.
- 4.11. Enforcement - Anyone found to have violated these policies may be subject to disciplinary action, up to and including termination of employment.

5.0 Responsibilities

- 5.1. The Infrastructure team is responsible for the review, revision and implementation of this policy and its associated procedures.
 - 5.1.1. This policy shall be reviewed and updated at least every two (2) years, and updated as required.

| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-151-000 ANTI-VIRUS POLICY | Original Issue Date: <u>01/18/2008</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|--|---|---|

ACKNOWLEDGEMENTS AND APPROVALS

The following have reviewed and approved this policy:

Originated/Revised by:

May 14 2012 4:26 PM

X

Dustin Bassler

Bassler, Dustin

Approved:

Jul 23 2012 11:54 AM

Apr 24 2012 4:12 PM

X

David Hobkins

Hobkins, David



X

Scott Kelly



Kelly, Scott

Revision History

| Revision Number | Date Revised | Approved By | Revision Description |
|-----------------|------------------|-------------|----------------------------------|
| <u>0</u> | <u>1/18/2008</u> | | <u>Original document.</u> |
| <u>9.01</u> | <u>8/26/2009</u> | | <u>Signature blocks updated.</u> |

| | | |
|--|---|---|
|   | DPL STANDARD OPERATING PROCEDURE POL-151-000 ANTI-VIRUS POLICY | Original Issue Date: <u>01/18/2008</u> Revision Number: <u>9.04</u> Last Revision: <u>4/9/2012</u> |
|--|---|---|

| | | | |
|-------------|------------------|--|--|
| <u>9.02</u> | <u>8/16/2010</u> | | Titles removed in section 4.5 and 5.1. Section 4.6 quarterly changed to weekly and real time scanning removed for Windows servers. |
| <u>9.03</u> | <u>1/6/2012</u> | | <u>Acknowledgements and approvals updated. Changed review timeline from "annually" to "every two (2) years."</u> |
| <u>9.04</u> | <u>4/9/2012</u> | | <u>Updated 5.1 language, added CoSign signature blocks.</u> |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | | |
|--|---|---|
|   | <p align="center">DPL STANDARD OPERATING PROCEDURE</p> <p align="center">POL-151-000</p> <p align="center">ANTI-VIRUS POLICY</p> | <p>Original Issue Date: <u>01/18/2008</u></p> <p>Revision Number: <u>9.04</u></p> <p>Last Revision: <u>4/9/2012</u></p> |
|--|---|---|

Annual Review:

Jul 26 2012 11:06 AM

X

Fuller, Jeffrey K.



Intrusion Protection System Policy

Original Issue Date:
9/26/2011

DPL Business Practice

159-101

Next Revision:
31-Oct-2012

Revision Number: 1

Intrusion Protection System Policy

REFERENCES

| <u>APPLICABILITY</u> | <u>TYPE</u> | <u>SENSITIVITY</u> |
|--|--|---------------------------|
| Corporate | Policy | Proprietary |
| <u>COMPLIANCE</u> | | |
| [Check all that apply] | | |
| <input type="checkbox"/> FERC Code of Conduct <input type="checkbox"/> NERC Reliability Standards <input type="checkbox"/> NERC Compliance <input type="checkbox"/> NERC Data Confidentiality <input type="checkbox"/> SOX | <input type="checkbox"/> PUCO Code of Conduct <input type="checkbox"/> PUCO CAM <input type="checkbox"/> PUCO Reliability Compliance <input checked="" type="checkbox"/> Other (please specify): Business Protection <input checked="" type="checkbox"/> None | |

DESCRIPTION**1 Purpose**

This policy outlines the methodology that will be utilized to monitor and inhibit malicious activity on the corporate and contractor networks.

2 Persons Affected

This policy applies to all corporate, contractor and internet network traffic.

3 Definitions

DPL – The operating divisions of both DPL Inc. and the Dayton Power and Light Company (DP&L).

IPS – The Intrusion Prevention Solution used to detect and prevent unsafe network traffic.

Rule Sets – A group of IPS filters used to permit, block, quarantine, or throttle network traffic.

Corporate network – DPL's corporate wired or wireless network utilized by corporate employees to facilitate computer activity.

Contractor network – Contractor's wired or wireless network utilized by contracted employees or their designees to facilitate work utilizing DPL-provided network and internet services.

ESS – Enterprise Security Services division of DPL.



Intrusion Protection System Policy

4 Policy

DPL shall utilize an IPS system to automatically detect, identify, inhibit and block unsafe network traffic on the corporate and contractor network. The IPS system shall be managed and maintained by the ESS Team.

5 Filtering

IPS filtering shall take place at all internet demarcation points of the corporate and contractor network. Filter monitoring shall be managed by the ESS Team. Additional IPS filtering shall take place within the corporate and contractor network as dictated by the ESS Team based on known or suspected nefarious or malicious information and/or activity.

6 Reports

ESS personnel shall provide weekly summary reports of unsafe activity filtered by the IPS system to ESS management.

- a. Access to IPS detail reports are considered confidential and must be requested and approved for distribution through ESS management.

7 Prevention

The IPS system shall actively drop and remove traffic deemed unsafe based on IPS system settings, rule sets, and interpretation by the ESS Team.

- a. ESS shall request the assistance of other IT support personnel when responding to IPS alerts and activity as needed particularly involving members or personnel responsible for Firewall activities.

8 Updates

IPS rule sets are actively modified and maintained by the ESS Team based on current traffic patterns and known malicious traffic activity.

- a. Minor updates to rule sets are performed in real-time as necessary. This is to facilitate the most current IPS rules sets are available for securing the corporate and contractor network from malicious activity without delay.
- b. Major updates and upgrades to rule sets are coordinated through DPL's IT Department CAB process and scheduled accordingly.
- c. IPS systems utilizing automatic rule set updates (similar to anti-virus definition updates) are performed automatically during non-business hours unless dictated under section 8.a.



Intrusion Protection System Policy

9 Enforcement

Corporate or contractor network users and computers facilitating unsafe network traffic shall be actively blocked from the network by the IPS system automatically or manually as dictated by the ESS Team. At no time shall any network user, corporate or contractor, attempt to circumvent any protective measures.

- a. Repeated enforcement of this policy shall be reported to the appropriate management, user's manager or in the case of a contractor the responsible DPL sponsor and HR and may lead to disciplinary action, up to and including termination of employment.

10 Review

This policy shall be reviewed and updated at least annually.

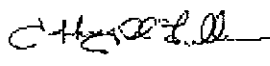
11 References and Attachments

None.

ACKNOWLEDGEMENTS AND APPROVALS

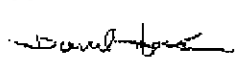
The following have reviewed and approved this policy:

Originated/Revised by:

 Fuller, Jeffrey K.
Sr. Manager Enterprise Security
Oct 7 2011 7:47 AM

Date:



Approved:

 Hoskins, David
Oct 7 2011 8:45 AM

Date:

REVISION HISTORY

| Revision Number | Date Revised | Approved By | Revision Description |
|-----------------|--------------|-------------|----------------------|
| | | | |

| | | |
|--|---|---|
|   | DPL Business Practice POL-159-202 Wireless Security Policy | Original Issue Date: <u>04/30/2012</u> Revision Number: <u>1</u> Last Revision: <u>1/07/2013</u> |
|--|---|---|

REFERENCES

| <u>APPLICABILITY</u> | <u>TYPE</u> | <u>SENSITIVITY</u> |
|---|--|---------------------------|
| Corporate | Policy | Public |
| <u>COMPLIANCE</u> | | |
| [Check all that apply] | | |
| <input type="checkbox"/> FERC Code of Conduct <input type="checkbox"/> NERC Reliability Standards <input type="checkbox"/> NERC Compliance <input type="checkbox"/> NERC Data Confidentiality <input checked="" type="checkbox"/> SOX | <input type="checkbox"/> PUCO Code of Conduct <input type="checkbox"/> PUCO CAM <input type="checkbox"/> PUCO Reliability Compliance <input checked="" type="checkbox"/> Other [please specify]: IT Business Policy <input checked="" type="checkbox"/> PCI | |

DESCRIPTION**1.0 Purpose**

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to any DPL network. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Enterprise Security Manager or Chief of Information (CIO) is approved for connectivity to DPL's networks.



Wireless networks are installed for convenience and as a complement to the wired network. Wireless networks provide shared bandwidth that does not provide performance of a wired switched network. Wireless networks are not intended to replace the wired networking that is required as part of the DPL's networking standards.

2.0 Scope

This policy covers all wireless data communication devices physically connected to any of DPL's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without connectivity to DPL's networks do not fall under the purview of this policy.

3.0 Policy

This Wireless Usage Policy applies to all workstations, notebooks, wireless local area networks, systems, servers and software applications used on DPL's network. It also applies to all employees, contractors, and visitors at DPL locations. The purpose of this policy is to ensure the security, reliability and utilization of the wireless network.

| | | |
|--|---|---|
|   | DPL Business Practice POL-159-202 Wireless Security Policy | Original Issue Date: <u>04/30/2012</u> Revision Number: <u>1</u> Last Revision: <u>1/07/2013</u> |
|--|---|---|

General Use

It is the intention of DPL to provide a high level of reliability and privacy when using the wireless network. Wireless access points provide a shared bandwidth and as the number of users increase the available bandwidth per user decreases. Users are asked to be considerate of others and refrain from running high bandwidth applications and operations such as downloading large files and video from the internet. DPL reserves the right to block access to sites that are identified as utilizing high bandwidth or containing malicious content.

DPL cannot guarantee the confidentiality of any information stored on any device connected to the DPL Wireless Network; therefore the wireless network should not be used to transmit critical and sensitive information such as social security and credit card numbers. Individuals assume full responsibility for their actions.

Security - General

Generally, eavesdropping on any DPL network communication (wired or wireless) is a violation of the DPL Acceptable Use and Wireless Usage policies.

All computers connected to the DPL network whether owned by the employee, contractor, guest or DPL, must be running approved anti-virus software with current signature files.



For security and network maintenance purposes, DPL may monitor individual equipment, or wireless network traffic at any time. DPL reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

DPL has the authority to disconnect any device from the wireless network that violates the practices set forth in this policy or any other related policy. It is the responsibility of the user to be knowledgeable of the information set forth in such policies.

All Authorized Users, Contractors and Guests are responsible for the following:

1. Adhering to established networking guidelines and policies.
2. Implementation of security software (antivirus, firewalls), patches and protocols on all equipment used to access the DPL Wireless Network.
3. Compliance with all policies and procedures and local and state laws pertaining to the security of sensitive and confidential data on the DPL networks.
4. Reporting known violations of the wireless network and all related equipment to Enterprise Security.

3.1 Access Points

| | | |
|--|---|---|
|   | DPL Business Practice POL-159-202 Wireless Security Policy | Original Issue Date: <u>04/30/2012</u> Revision Number: <u>1</u> Last Revision: <u>1/07/2013</u> |
|--|---|---|

All wireless Access Points / Base Stations connected to the network must be registered and approved by DPL IT and Enterprise Security. All approved Access Points / Base Stations are subject to periodic penetration tests and audits.

3.2 Approved Technology

All wireless LAN hardware implementations shall utilize Wi-Fi certified devices that are configured to use the latest security features available. DPL reserves the right to not allow or disconnect any device that doesn't meet a minimum set of requirements.

3.3 Physical Location

Security mechanisms should be put in place to prevent the theft, alteration, or misuse of Access Points / Base Stations. All devices shall be locked and secured in an appropriate manner.

3.4 Configuration

The default SSID and administrative username / password shall be changed on all Access Points / Base Stations. Device management shall utilize secure protocols such as HTTPS and SSH. If SNMP is used in the management environment, all default SNMP community strings must be changed or otherwise disabled. If configurable, remove SSID broadcast, or at a minimum adjust the SSID beacon transmission rate to the highest value. Console access shall be password protected.

3.5 Authentication and Transmission



All wireless access points that connect clients to the corporate network (DPLinc) shall require certificates that will be used to provide unique authentication over secure channels and all data transmitted shall be encrypted with an approved encryption technology.

Users of the guest network will be required to provide either a short term user name and password, or a unique user name and password combination to gain access to the network. All data transmitted on the guest network shall be encrypted with an approved encryption technology

3.6 Internet-only Deployment

Access Points / Base Stations deployed to provide Internet-only service shall be separated from the internal network by denying all internal services. Access Point / Base Station management shall be limited to internal or console users and not available to wireless clients.

4.0 Enforcement

| | | |
|--|---|---|
|   | <p align="center">DPL Business Practice</p> <p align="center">POL-159-202</p> <p align="center">Wireless Security Policy</p> | <p>Original Issue Date: <u>04/30/2012</u></p> <p>Revision Number: <u>1</u></p> <p>Last Revision: <u>1/07/2013</u></p> |
|--|---|---|

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment and may be subject to criminal prosecution under state and federal laws.



Definitions

| Term | Definition |
|-----------------|--|
| HTTPS | Hypertext Transfer Protocol over Secure Socket Layer is a URL scheme used to indicate a secure HTTP connection. |
| SNMP | Simple Network Management Protocol is used in network management systems to monitor network attached devices for conditions that warrant administrative attention. |
| SSH | Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two computers. |
| SSID | Service Set Identifier is a name used to identify the particular 802.11 wireless LAN to which a client wants to attach. |
| Wi-Fi Certified | Wi-Fi certified is a program for testing products to the 802.11 industry standards for interoperability, security, easy installation, and reliability. |

5.0 Responsibilities

The Enterprise Security Services Manager is responsible for the review, revision and implementation of this policy and its associated procedures.

This policy shall be reviewed at least every two (2) years and updated as required.

| | | |
|--|---|--|
|   | DPL Business Practice POL-159-202 Wireless Security Policy | Original Issue Date: <u>04/30/2012</u> |
| | | Revision Number: <u>1</u> Last Revision: <u>1/07/2013</u> |

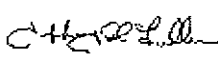
ACKNOWLEDGEMENTS AND APPROVALS

The following have reviewed and approved this policy:

Originated/Revised by:



Chip Wenz Wenz, William
 Security Analyst II
 Jan 8 2013 9:18 AM

Approved:

 Fuller, Jeffrey K.
 Sr. Manager, Enterprise Security
 Jan 8 2013 9:21 AM

Revision History

| Revision Number | Date Revised | Approved By | Revision Description |
|-----------------|--------------|-------------|--|
| 0 | 04/30/2012 | | Original Document |
| 1 | 1/07/2013 | | Updated to reflect the installation of the new corporate and guest wireless networks |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | | |
|--|---|--|
|   | DPL Business Practice POL-159-202 Wireless Security Policy | Original Issue Date: <u>04/30/2012</u> |
| | | Revision Number: <u>1</u> Last Revision: <u>1/07/2013</u> |

Annual Review:

Information Technology – Exhibit 3

List of Information Technology Capital Initiatives for 2016

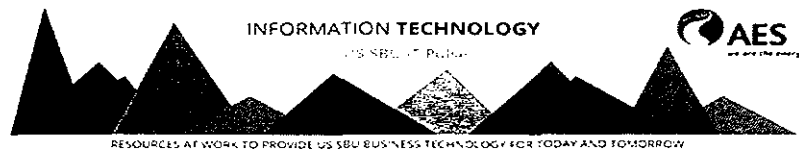
| Category | Initiative | Amount |
|----------|--|---------------|
| DPL | US SBU ERP Consolidation DPL | \$ 12,550,000 |
| DPL | DPL Replacement of telephony system, including IVR | \$ 1,722,460 |
| DPL | DC Strategy DPL | \$ 1,707,437 |
| DPL | CSS PUCO Enhancements (includes Net Metering Phase I & II, e | \$ 1,200,000 |
| DPL | DPL Oracle DB Upgrade | \$ 814,540 |
| DPL | DPL Web Portal For Customer Self-Service Phase 3 | \$ - |
| DPL | DPL Web Portal For Customer Self-Service Phase 2 | \$ 698,466 |
| DPL | DPL Web Portal for Customer Self-Service Phase 1 | \$ 600,000 |
| DPL | PC Life Cycle DPL | \$ 500,000 |
| DPL | Network Infrastructure - Lifecycle | \$ 400,000 |
| DPL | VOIP DPL | \$ 360,500 |
| DPL | DPL Server Infrastructure (Non-discretionary) | \$ 250,000 |
| DPL | DPL Oracle WebCenter Upgrade | \$ 215,448 |
| DPL | DPL FCS Application Upgrade (life cycle) | \$ 201,568 |
| DPL | DPL US SBU Active Directory Integration | \$ 200,000 |
| DPL | DPL Telecom Enhancements - Lifecycle | \$ 170,000 |
| DPL | DPL Telepresence | \$ 150,000 |
| DPL | DPL CSS MOM Enhancements | \$ 145,520 |
| DPL | USPS Addressing in CSS | \$ 135,760 |
| DPL | SharePoint DPL | \$ 135,000 |
| DPL | Tariff Modeler - Lifecycle | \$ 90,721 |
| DPL | DPL MV90 Upgrade (life cycle) | \$ 87,992 |
| DPL | DPL CSS Collection Agency DebtNext | \$ 77,662 |
| DPL | DPL CSS Collections CSC Enhancements | \$ 65,578 |
| DPL | DPL Incident Management | \$ 54,000 |
| DPL | DPL Portableviewer - Geoview DPL ESRI License Purchase for € | \$ 50,000 |
| DPL | DPL Energy Vision Technology Upgrade (life cycle) | \$ 45,200 |
| DPL | LANDesk (Workspaces) DPL | \$ 45,000 |
| DPL | DPL Encryption | \$ 23,400 |

Information Technology – Exhibit 4

Information Technology Mission Statement

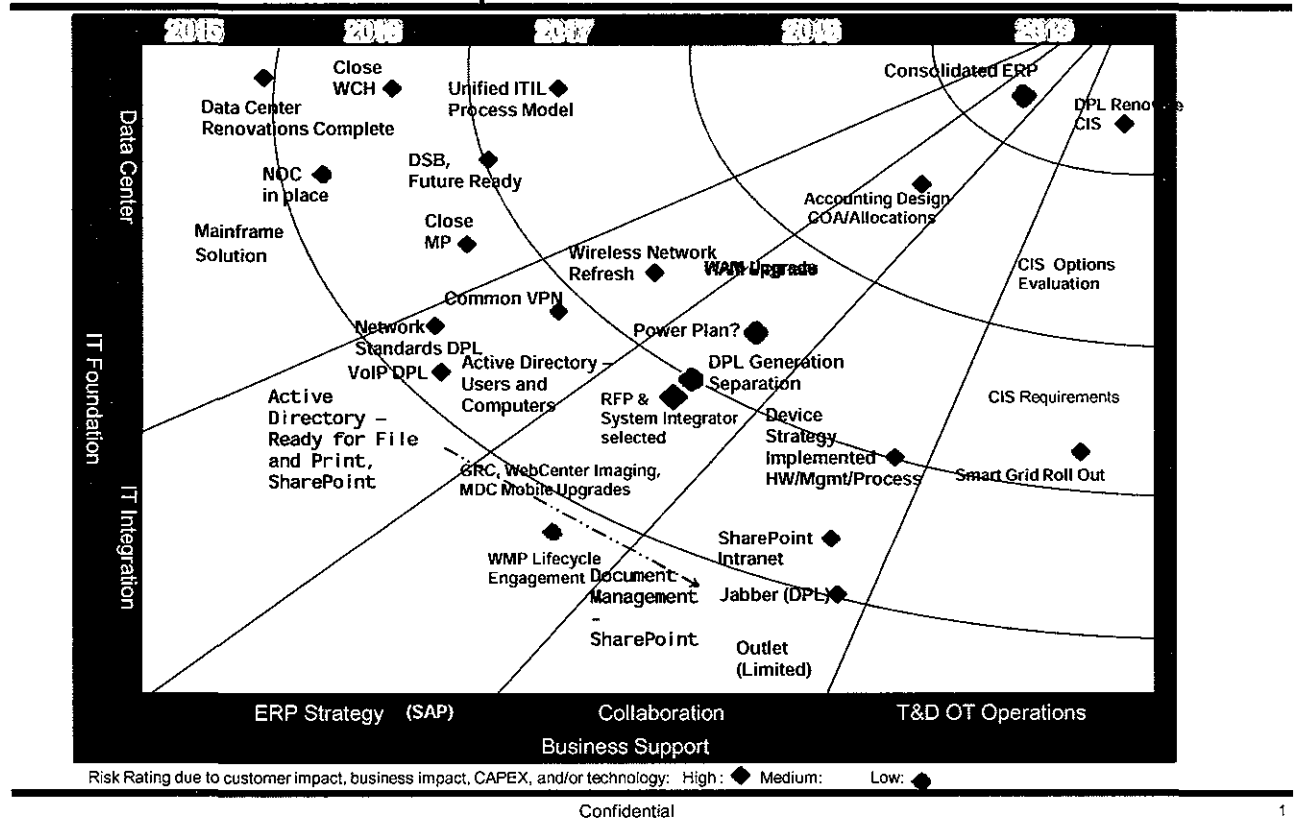
US SBU IT Mission

Provide a standardized and integrated information technology platform that enables us to access services, tools and solutions that are reliable, scalable, secure, productive and increases efficiency of our US SBU people.



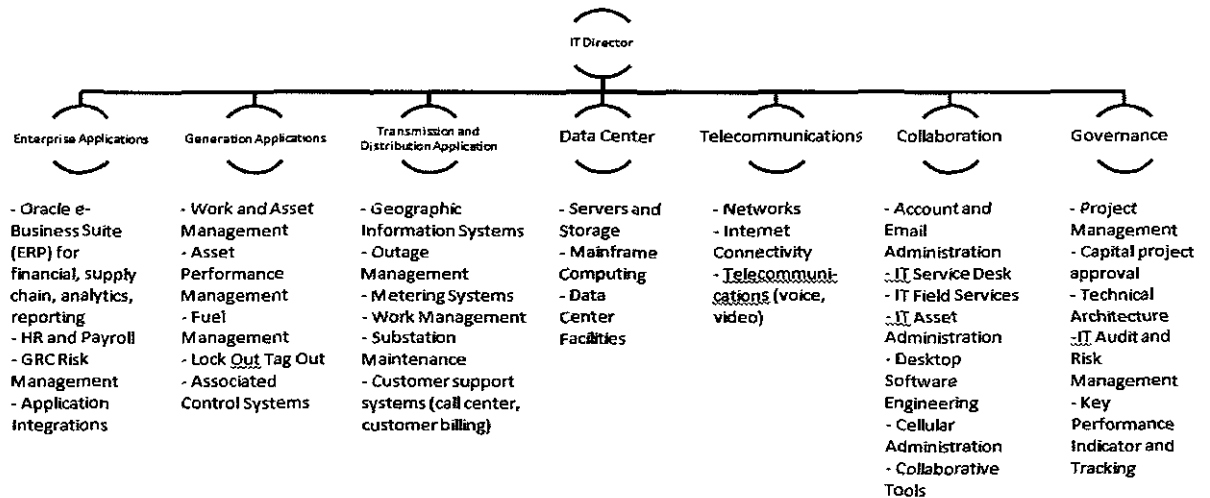
Information Technology – Exhibit 5

Information Technology Transformation Roadmap 08-October-2015

**IT Transformation Road Map DPL 10-8-2015**

Information Technology – Exhibit 6

Organizational Structure of Information Technology



Information Technology – Exhibit 7


Timeline of Recent Customer Service System Modifications and Enhancements

| | | |
|-----------|--|---|
| 2009 | E-Mail Address and Cell Phone Information | Billing system storage of customer E-mail addresses, cell phone numbers, and various flags to denote appropriate usage. |
| 2009 | Rate Changes | Implementation of several riders, such as the Alternative Energy Rider, Economic Development Rider, Transmission Cost Recovery Rider, etc. |
| 2009 | Energy Efficiency Discount Program | Implementation of the energy efficiency discount program for mercantile customers. |
| 2009 | Payment Plan Changes | Addition of a 1/9th payment plan and modifications to the 1/3rd payment plan as required by OAC 4901:1-18. |
| 2009-2010 | Economic Development Programs | Implementation of six new economic development programs as required by Senate Bill 221. |
| 2009-2012 | PIPP Reform | Implementation of changes necessary to comply with a revised Percentage of Income Payment Plan that is regulated by the Ohio Development Services Agency. |
| 2010 | Fuel Fund | Enhancement of the billing system to post and track fuel fund credits. |
| 2011 | Payment Posting Priorities | Modified billing system to reflect changes in payment posting priorities related to deposits and other miscellaneous charges. |
| 2011 | Non-Pay Disconnection Notice | Implementation of changes in collection processing timeline. |
| 2011 | Governmental Aggregation | Enhanced billing system to handle governmental aggregations for competitive retail electric supply (CRES) providers. |
| 2011-2012 | Capacity and Transmission Obligations | Enhancement of the billing system to save capacity and transmission obligation amounts for each customer and provide information to CRES providers. |
| 2011-2012 | Bill-Ready Billing for CRES Providers | Implementation of bill-ready consolidated billing for CRES providers. |
| 2012 | Courtesy Non-Pay Disconnection Notice | Modification of the billing system to produce 13-day disconnection notice if 14-day notice is rendered in winter through April 15. |
| 2012 | Meter Reading Trouble Codes | Implementation of additional meter reading trouble codes. |
| 2012 | Social Security Numbers | Implementation of audit tracking of SSN viewing. |
| 2012-2013 | IVRU Customer Self-Service | Implementation of changes to IVRU to provide customers with more robust self-service options. |
| 2013 | E-Bill Indicator | Addition of an indicator that customer is using E-billing. |

| | | |
|-------------|--|---|
| 2013 | Accounts Receivable Reporting | Enhancement of accounts receivable reporting from the billing system. |
| 2013 | Mobile Order Management Upgrade | Implementation of changes in billing system for Mobile Order Management System upgrade. |
| 2013 | ESP Rates | Implementation of rates resulting from the Electric Security Plan. |
| 2013 | Standard Sync List | Standardization of sync list to ensure identification of the correct accounts that are served by each CRES provider. |
| 2014 | Switching Fees | Implementation of changes to suppress billing customers for switching fees. |
| 2014 | Auto-Cancellation for Bill-Ready Billing | Implementation of automatic cancellation of CRES provider charges when DP&L charges are cancelled. |
| 2014 | Historical Interval Usage | Support historical interval usage data requests via electronic data interchange (EDI). |
| 2014 | % Off Price-to-Compare | Implementation of calculation of a percentage off the "Price-to-Compare" as a CRES provider pricing option. |
| 2014 | Shopping on a Per Meter Basis | Implementation of validation to ensure non-residential and residential meters are not on the same bill account. |
| 2014 | Interval Meter Threshold Requirement | Implementation of change to interval meter requirement (from $\geq 100\text{kW}$ to $> 200\text{kW}$) for switching to a CRES provider. |
| 2014 | Meter Reading Source Record | Enhancement to create orders to enable change of meter reading source record from interval to non-interval. |
| 2014 | Supplier Default | Implementation of changes to accommodate a supplier default and mass return to standard service offer. |
| 2014-2015 | Web Portal for CRES Provider Self-Service | Implementation of a web portal for CRES providers to obtain customer usage data, EDI testing requirements, supplier information, required forms; enter pricing option additions and changes, etc. |
| 2015 | Guarantor Agreements | Implementation of changes to timelines, disconnects, correspondence, and deposits related to guarantor agreement OAC changes. |
| 2015 | Debit/Credit Transfers | Implementation of changes to final bill transfers and landlord agreements to ensure transfer of debits and credits can only be made to like-service accounts. |
| 2015 | Bill Format Re-Design | Implementation of re-designed customer bill format. |
| 2015 | ODSA PIPP Rule Changes | Modifications to PIPP processing due to OAC changes. |
| In Progress | Tariff Modeler Upgrade | Upgrade of tariff builder and rating engine for the billing system. |
| In Progress | Web Portal for Customer Self-Service | Enhancements to website for customer self-service. |

Information Technology – Exhibit 8

Competitive Retail Electric Service Provider Portal



[Login](#)
[User Name](#)
[Forgot Password?](#)

[Password](#)
[Sign In](#)

DP&L Electric Choice Suppliers

General Information for potential DP&L Electric Choice Suppliers

[Home](#)
[About Us](#)
[Contact Us](#)
[FAQs](#)
[AGS Load Information](#)
[Capacity and Transmission](#)
[SD Information](#)
[FAQs](#)
[Interval Meters](#)
[Schedules](#)
[Supplier Handbook](#)
[Supplier Registration Materials](#)
[Rates and Rate Index](#)

[Search](#)

Supplier Information

Information for current or potential suppliers

The Dayton Power and Light Company (DP&L) is pleased to share information with Competitive Retail Electric Service (CRES) Providers who currently serve, or would like to serve retail load within the certified territory of DP&L.

To ask questions regarding this site, its contents or the implementation of retail electric choice within DP&L's territory, please call the Retail Supplier Hotline between 8 a.m. and 5 p.m. (Eastern) or send us an email.

Supplier Hotline: 937-331-4431
E-mail: RetailSupplierInformation@dplinc.com or retail@eei.com

Access Levels II & III

Access to secure information on the site is reserved for CRES Providers who are certified with the Public Utilities Commission of Ohio (PUCO) or have already completed the Alternate Generation Supplier registration process with DP&L.

The following information is available only to users with certain minimum access levels:

- Level II (PUCO-Certified CRES Providers)
 - Historical Usage Portal
 - Pre-enrollment Customer List
 - Government Aggregation List
- Level III (DP&L Registered Suppliers)
 - Discount Rate Tool
 - Manage Pricing Options Portal
 - Payment Agreement List
 - Supplier Agreements
 - Sync List

Click [Need Help?](#) to learn how to obtain login credentials.

Disclaimer: Use of any of the information provided through this site is not required. While DP&L endeavors to maintain a high degree of accuracy with respect to its data, errors can occur for a variety of reasons and may not be identified or corrected. DP&L is not making this information available for any particular purpose and makes no representations or warranties regarding the accuracy of the information, the degree or frequency of updates, the use of this information or conclusions that may result from use of this information. The user hereby accepts full responsibility for any action or forbearances undertaken based on or in connection with use of this information. The user hereby releases and discharges DP&L from any liability, and agrees to indemnify and hold DP&L harmless from any costs, expenses, or liabilities by DP&L, user or any third party, arising from or relating to the user's use of the provided information and tools.


The Dayton Power & Light Company
 Attn: Control Area Services
 1900 Dryden Rd
 Dayton, Ohio 45439

You may also contact us by:
 Email:
RetailSupplierInformation@dplinc.com
 Fax:
 (937) 331-4216

Retail Supplier Hotline:
 (937) 331-4431

[Site Index](#)
[Contact DP&L](#)
[CRES Portal Terms of Use](#)
[DP&L's Privacy Policy](#)
[DP&L's Terms of Use](#)

© 2015 Dayton Power & Light. All Rights Reserved.
 Version 1.0.44.32878



Information Technology – Exhibit 9

Customer Service System Interfaces

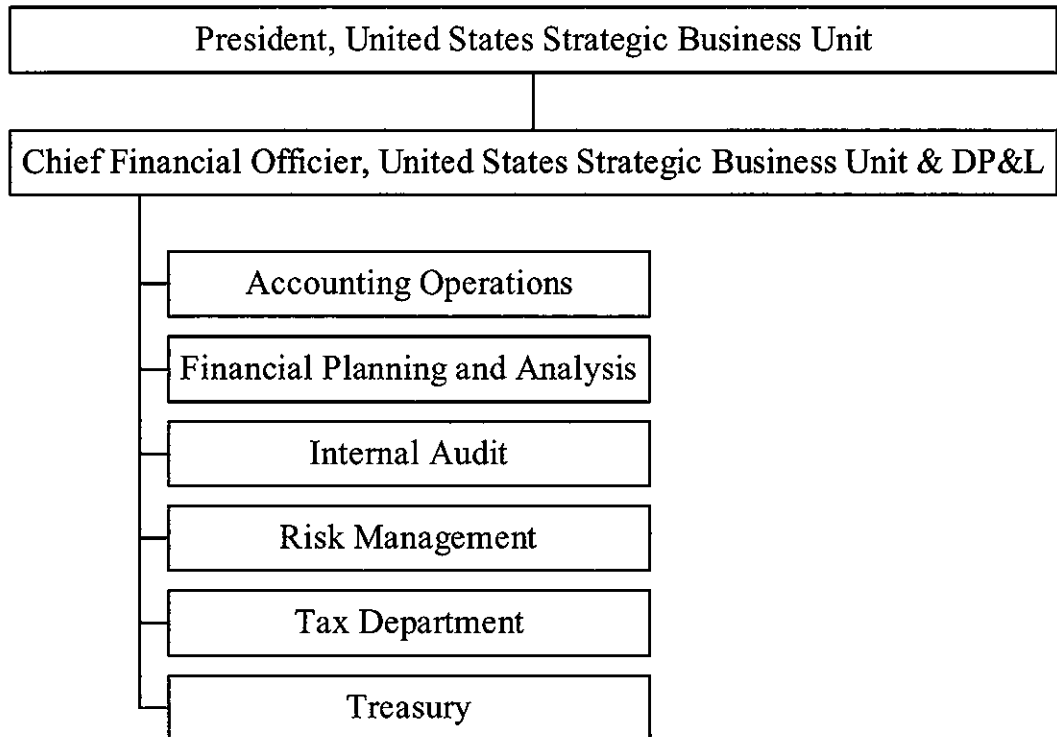
| Inputs to Customer Service System |
|---|
| Check Free – Automated Clearing House Payments |
| Fifth Third Bank – Lockbox |
| Firstech – Authorized Pay Agents |
| JPM Chase – Payment Consolidator |
| Mobile Order Management |
| MV 90 – Interval Meter Data |
| Scanned Cash – Check Scanning |
| Tariff Modeler |

| Outputs from Customer Service System |
|---|
| Datamart – Financial Data Repository |
| DocuLynx – Customer Service System Archive |
| Oracle – General Ledger |
| Trouble Call Management System |

| Two-Way interface with Customer Service System |
|---|
| Collection Agencies |
| CRES Portal |
| Customer Portal |
| EC Suppliers – Electronic Data Interchange |
| EnergyVision – Settlement System |
| Interactive Voice Response Unit |
| Itron – Field Collection System |
| Ohio Development Services Agency |
| Oracle – Accounts Payable |
| SourceLink – Bill Print and E-Bill |
| Speedpay – Electronic Payments |

Office of DP&L's Chief Financial Officer

Finance is responsible for ensuring that DP&L has the financial security needed to support its primary mission of providing reliable and affordable electric service. The functions provided by Finance are described in detail in the following sections.



Functional Area:
Accounting Operations

SFR Reference
(B)(9)(b)(ii) Accounting systems and financial reporting

Policy and Goal Setting:

The US SBU Controllers Group provides accounting services to DP&L. The policies that govern the team's activities include adaptation of policies issued by AES Corporate as well as those prepared by Accounting Operations for activities unique to DP&L. The US SBU Policy Committee approves all policies that govern US SBU-wide activities such as travel and entertainment, while the US SBU CFO has the authority to approve policies that only impact the Finance organization, such as setting timing requirements for account reconciliation review and approval. These policies are designed to reflect enterprise practices as well as industry standards and requirements. They are available electronically to all employees via a link installed on all US SBU desktops. The policies and a strong internal control environment are designed to ensure the timely and accurate preparation of internal and external reports, which is one of Accounting Operations primary and enduring goals. In a process led by the US SBU Controller, all goals for Accounting Operations are set annually in alignment with the US SBU-wide business plan, which drives the components of the US SBU CFO's tactical plan.

Strategic and Long-Range Planning:

The US SBU Senior Leadership Team is responsible for establishing the US SBU business plan, discussed above in the "Policy and Goal Setting" section, which includes long-range financial and operational planning.

Organizational Structure and Responsibilities:

DP&L's accounting is provided by the US SBU Accounting Operations, one of several centralized shared service areas that also provides support to several other entities that are part of the US SBU, including Indianapolis Power & Light. The US SBU Controller, who leads Accounting Operations, reports directly to the US SBU CFO and has a dotted line reporting relationship to the AES Corporate Controller.

The accounting departments that report to the US SBU Controller include Technical, General, Operations, Regulatory, Revenue, Fixed Assets Accounting, as well as Financial Reporting, Payroll, Accounts Payable and Financial Controls. Labor costs for services provided to DP&L are either directly charged to DP&L or directly charged to a project number that results in a distribution among the appropriate combination of entities based on the individual's standard work load split.

Key responsibilities of each of the departments within the US SBU Accounting Operations are as follows:

1. Technical Accounting
 - a. Contract review
 - b. New accounting pronouncement analysis and implementation assistance
 - c. Accounting guidance interpretation as requested
2. General Accounting
 - a. Oversee the closing of the books and records monthly timely and accurately
 - b. Assist in preparation of accounting-related data in support of initiatives and activities of the other teams within Accounting Operations
3. Operations Accounting
 - a. Prepare journal entries related to the operations of generation facilities that are owned jointly with third parties
 - b. Coordinate the capture and monthly allocation of costs incurred by the Service Company on behalf of DP&L
 - c. Prepare monthly occupancy cost allocations to entities who benefit from the use of space owned by DP&L
4. Regulatory Accounting
 - a. Prepare accounting related schedules for various routine filings with the PUCO, as well as the related journal entries
 - b. Coordinate the preparation of DP&L's quarterly FERC 3Q's and annual FERC Form 1
 - c. Prepare testimony and schedules related to general rate cases as necessary
5. Revenue Accounting
 - a. Record revenues related to DP&L, including the monthly unbilled revenue calculation
 - b. Provide internal management reporting and analysis for revenue results
 - c. Provide billing service for miscellaneous utility and certain non-utility services
6. Fixed Assets Accounting
 - a. Maintain property records, including depreciation, AFUDC and ARO
 - b. Provide guidance on capital versus expense accounting
 - c. Prepare asset related rate case exhibits
7. Financial Reporting
 - a. Coordinate data gathering for preparation of SEC Form 10-Q's and 10-K
 - b. Preparation of formal financial statements, including footnotes
 - c. Obtain review input from the DP&L Disclosure Committee, Board of Directors and the independent external auditors

- d. Prepare monthly and quarterly analysis to explain trends and variances compared to prior periods
 - e. Support rate case activity
- 8. Payroll
 - a. Coordinate the processing of timecards and payroll payments
 - b. Preparation of monthly, quarterly and annual payroll reporting to government agencies
- 9. Accounts Payable
 - a. Maintenance of vendor master file
 - b. Timely processing of invoice payments
 - c. Compliance with regulations and company policies
- 10. Financial Controls
 - a. Coordination of annual control self-assessment testing
 - b. Assistance on control deficiency mitigation
 - c. Assistance on preparation of policies and procedures
 - d. Control-related interaction with independent external and internal auditors

The organizational chart for Accounting Operations is attached as Accounting Operations - Exhibit 1.

Decision-Making and Control:

The US SBU Controller provides overall direction to the members of Accounting Operations, with individuals throughout the organization making decisions within their scope of authority in support of DP&L's overall mission and in accordance with the DP&L policies and procedures. The primary function of the US SBU Accounting Operations relates to the proper disclosure of accounting and financial data to satisfy external regulations and requirements. Quality control over the preparation of documents filed quarterly and annually with the SEC include reviews by the DPL Disclosure Committee and Board of Directors, as well as the independent external auditors which includes their formal audit opinion for the SEC Form 10-K. Subject matter experts throughout the US SBU assist with the preparation and review of the quarterly and annual financial filings with the FERC, with the annual FERC Form 1 audited by the independent external auditor. In addition, the Internal Audit Department conducts reviews of accounting activity and adherence to policies and procedures. The Internal Audit annual audit plans are designed to focus on areas selected by them and as requested by senior management of the US SBU as well as the DP&L Board of Directors.

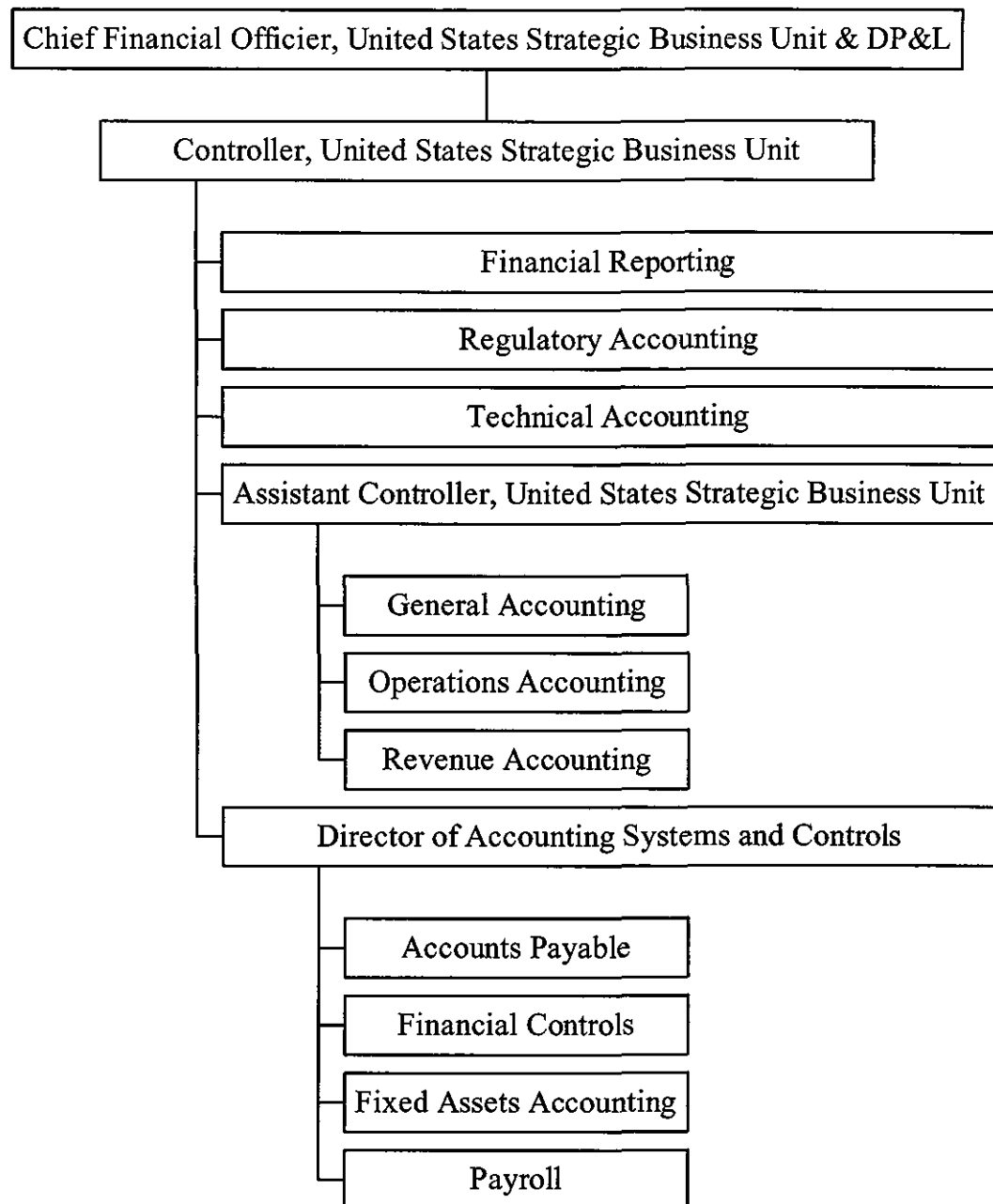
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including: phone calls, conference calls, face to face meetings and e-mail. Internal communications typically correspond to interaction between the departments within the US SBU Accounting Operations and with the other functions that report to the US SBU CFO that is necessary to provide DP&L with accounting and financial reporting support. Communication with operational areas is also required to gather necessary information.

External communications are accomplished through a variety of communication channels including: phone calls, conference calls, telepresence, meetings, and e-mail. Communications typically involve interaction with DP&L's external auditors, joint owners of the generation fleet, vendors and members of the AES Corporate team.

Accounting Operations – Exhibit 1

Organizational chart for Accounting Operations



Functional Area:
Financial Planning and Analysis

SFR Reference
(B)(9)(b)(iii) Budgeting and forecasting
(B)(9)(b)(iv) Financial planning process and objectives

Policy and Goal Setting:

Financial Planning and Analysis supports the overall corporate financial policies and the corporate policies embodied in the AES code of conduct, which establishes the guidelines by which DP&L employees are expected to conduct business. The Company's financial policies are the responsibility of the CFO.

The first priority of all DP&L areas is to ensure the safety of all DP&L employees, contractors and the public. Financial Planning and Analysis supports this effort by holding monthly safety meetings and by financially supporting operational efforts intended on making DP&L a safer place to work.

The annual goals and objectives of Financial Planning and Analysis are designed to support the achievement of DP&L's business plan. These goals and objectives are supported by one common goal: meeting or beating expectations based on internal goals and external public earnings guidance which are approved by the CFO.

Strategic and Long-Range Planning:

DP&L's strategic direction is established by senior management. Financial Planning and Analysis address the needs of senior management by providing financial analysis of various strategic and financial direction options prior to decisions being made. Once a strategic direction is identified, communication and coordination among many departments occurs to build DP&L's annual financial plan. Various updates to this plan are made before a finalized financial plan is approved.

Organizational Structure and Responsibilities:

The Financial Planning and Analysis Department consists of 1 manager and 2 analysts who are led by the Director of Financial Planning and Analysis. Financial Planning and Analysis is primarily responsible for the preparation of DP&L's annual financial plan, which includes short-term and long-term (next 10 years) operating and cash forecasts. Financial Planning and Analysis also assists Corporate Accounting in monitoring corporate budget variances and provides variance explanations to senior management. The forecasts are used to assist in the development of DP&L and its subsidiaries' strategy for regulatory and competitive issues.

Other activities performed by Financial Planning and Analysis include:

1. Short-term and long-term financial analysis
2. Strategic and corporate planning support and scenario analysis
3. Rating agencies presentations and support
4. Provide data utilized by Regulatory Operations for rate filings
5. Provide rate planning and testimony support
6. Provide economic and financial decision-making support, through the project expenditure approval process
7. Support the Corporate AES team and senior management review process
8. Develop and update forecast models and methodologies to incorporate changes in business
9. Assist in the accounting month-end close procedures, through the variance reporting process

The organizational chart for Financial Planning and Analysis is included as Financial Planning and Analysis - Exhibit 1.

Decision-Making and Control:

Decision-making involves applying financial and economic evaluation methods, along with independent judgment, to the many financial and operating issues that impact DP&L. Most decisions are made on the reasonableness of data, comparing it to previous years, trend data, expected results based on analysis and forecasts of changes in the industry environment as well as other operating or financial considerations.

There is not one defined criterion utilized for decision-making purposes but rather criteria are driven by the issue being addressed. Financial Planning and Analysis staff make decisions within their given scope of authority in support of DP&L's overall mission and in accordance with the policies and procedures. Decisions are raised to the proper level of authority as required by DP&L's policies.

Much of the decision-making in Financial Planning and Analysis is iterative in that results of one analysis imply another analysis is necessary to validate assumptions or conclusions. These subsequent analyses are often provided to senior management for their review process.

Assumptions and analysis are reviewed by the Director of Financial Planning and Analysis for reasonableness and consistency in theory application.

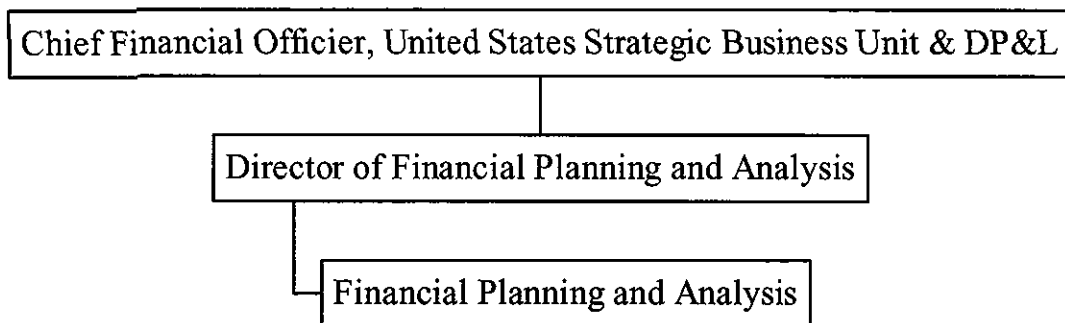
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including regular staff meetings, conference calls, telepresence and e-mail. Types of information shared within the department include directions and/or assumptions for a particular analysis,

brainstorming for problem resolution, relaying information and assignments, and communication of corporate direction from senior management.

Financial Planning and Analysis – Exhibit 1

Organizational Chart for Financial Planning and Analysis



Functional Area:
Internal Audit and Advisory Services

SFR Reference
(B)(9)(b)(vi) Internal auditing

Policy and Goal Setting:

DP&L's Internal Audit function is performed by the US SBU Internal Audit and Advisory Services group. The AES Corporation Internal Audit Charter governs Internal Audit and Advisory Services responsibilities and includes guidelines for the performance of related duties, independence, authority and accountability.

The mission of Internal Audit and Advisory Services is to provide independent, objective assurance and consulting services designed to add value, improve DP&L's operations, and comply with regulatory requirements in accordance with the Institute of Internal Auditors' "Code of Ethics" and the Institute's "International Standards for the Professional Practice of Internal Auditing." Internal Audit and Advisory Services helps the Company to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal controls, and governance processes.

Strategic and Long-Range Planning:

Risk based annual audit and advisory service plans are created in response to a formal risk analysis process initiated by AES Corporate and adopted locally by US SBU Internal Audit and Analysis Services. Following a series of interviews with team members of the US SBU executive leadership, an evaluation of key business risk factors is performed taking into account key process changes, system implementations, related industry trends and developments. The annual audit plan, comprised of operational, financial and information technology related audit projects is presented to the Audit Committee of the Board of Directors.

Organizational Structure and Responsibilities:

AES Corporate Internal Audit and Advisory Services is led by the Chief Audit Executive ("CAE") - in order to provide for the independence of the Internal Audit and Advisory Services group, its personnel located within each strategic business unit report to the CAE, who in turn reports functionally to the Audit Committee and administratively to the AES Chief Information Officer.

US SBU Internal Audit and Advisory Services is responsible for all US SBU related activities. The Director of Internal Audit and Advisory Services is responsible for all audit activities and reports directly to the CAE and the CFO.

Internal Audit and Advisory Services has an overall objective to ensure that the organization's network of risk management, control and governance processes as designed and represented by management is adequate and functioning properly. Internal Audit and Advisory Services has responsibility to:

1. Develop a flexible annual audit plan using an appropriate risk-based methodology, including any risks or control concerns identified by management, and submit that plan to the Audit Committee for review and approval as well as periodic updates
2. Implement the annual audit plan, as approved, including as appropriate any special tasks or projects requested by management and the Audit Committee
3. Oversee AES testing of internal controls to support management's annual assertions relating to the effectiveness of internal control over financial reporting as required under the Sarbanes-Oxley Act of 2002
4. Maintain and/or engage a professional audit staff or outside professional service provider with sufficient knowledge, skills, experience, and professional certifications to meet the charter requirements
5. Evaluate and assess significant merging/consolidating functions and new or changing services, processes, operations, and control processes that coincide with their development, implementation, and/or expansion
6. Issue periodic reports to the Audit Committee and management summarizing results of audit activities
7. Keep the Audit Committee informed of emerging trends and successful practices in internal auditing
8. Provide a list of significant measurement goals and results to the Audit Committee
9. At the request of management and/or the Audit Committee, assist in the investigation of significant suspected fraudulent activities within AES and notify management and the Audit Committee of the results
10. Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to the organization at a reasonable overall cost
11. Establish and maintain a quality assurance and improvement program to help ensure the internal audit responsibilities are carried out in an effective and efficient manner

Opportunities for improving management control, profitability, and AES's image may be identified during audits and advisory projects; these are communicated to the appropriate level of management for development and implementation of related action plans. Furthermore, a primary focus is also to ensure processes are adequate to provide required certifications related to internal controls.

The CAE, Directors and staff of the Internal Audit and Advisory Services group are authorized to:

1. Have unrestricted access to all functions, records, property, and personnel, other than searches of electronic mail, which must be approved by the Company's General Counsel
2. Have full and free access to the Audit Committee
3. Allocate resources, set frequencies, select projects, determine scopes of work, and apply the techniques required to accomplish audit objectives
4. Obtain the necessary assistance of personnel in the AES groups and businesses where they perform audits, as well as other specialized services from within or outside AES

The CAE, Directors and staff of the Internal Audit group are not authorized to:

1. Perform any operational duties for AES or its affiliates
2. Initiate or approve accounting transactions external to Internal Audit and Advisory Services
3. Direct the activities of any AES employee not employed by Internal Audit and Advisory Services, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors

While performing Internal Audit and Advisory Services activities, all staff are required and encouraged to keep safety as a top priority, and report any safety lapses to management promptly for responsive actions.

The organizational chart for Internal Audit and Advisory Services is included as Internal Audit and Advisory Services - Exhibit 1.

Decision-Making and Control:

Based on the annual audit plan, the Director of Internal Audit and Advisory Services provides overall guideline and responsibilities for audit and advisory projects performed during an audit year. Standard operating procedures have been developed for guidance around the conducting of audit and advisory assignments, these include:

1. Audit announcement
2. Audit planning
3. Fieldwork commencement
4. Closing/exit meeting
5. Initial draft report
6. Management response on draft report
7. Work paper review
8. Final draft report
9. Audit project closure
10. Report to Audit Committee

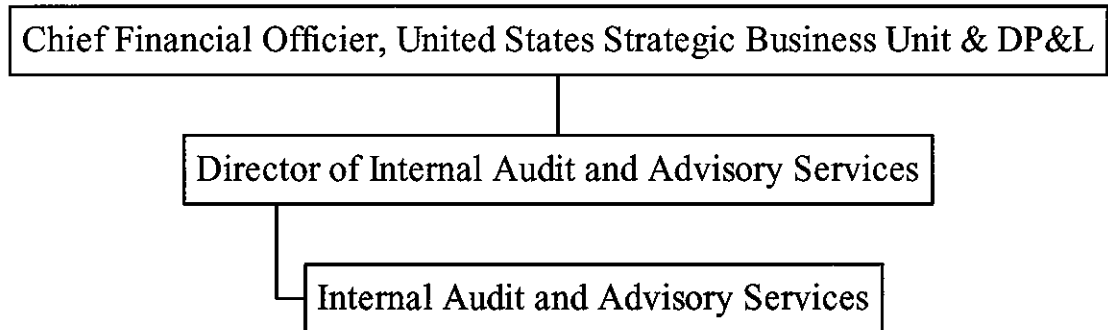
Further guidance is also available on sample selection for audit tests performed, materiality levels, and report ratings/conclusions.

Internal and External Communications:

Internal Audit and Advisory Services maintain a regular and continuous channel of communication with DP&L audit client personnel throughout on-going audit and advisory service assignment. Forms of internal communication include: face to face meetings, phone calls, conference calls, and email. Formal communication is issued at the time of audit kick-off, followed up by formal document and interview requests. Audit reports typically include an executive summary, scope summary, conclusion, audit finding, risk description, audit recommendations, and agreed action plans. In addition Internal Audit and Advisory Services provide periodic updates to the Audit Committee on current audits.

Internal Audit and Advisory Services – Exhibit 1

Organizational Chart for Internal Audit and Advisory Services



Functional Area:
Risk Management

SFR Reference
(B)(9)(b)(vii) Risk management
(B)(9)(e)(ii) Insurance

Policy and Goal Setting:

The US SBU has a Risk Management policy which governs the actions and risk taking within the US SBU. Policies and goals of Risk Management are established and executed consistent with the mission and values of the AES Corporation.

The first priority of all DP&L areas is to ensure the safety of all DP&L employees, contractors and the public. Risk Management supports these efforts by helping to maintain safety awareness through active participation in safety walks, safety meetings and DP&L's safety day.

Goal setting is determined using several metrics and/or tools such as enterprise risk management, conditional value at risk, volumetric hedging levels, and available collateral. Specific to Insurance, this typically centers on obtaining the most favorable risk transfer terms (either via contractual risk transfer or via insurance) at the most favorable cost. In addition, the annual budget process is where the overall financial objectives are outlined.

Strategic and Long-Range Planning:

Strategic and long-range planning for Risk Management is completed through collaboration of cross functional participation groups within the US SBU Risk Management Committee ("RMC"), AES Corporate Risk Oversight Committee as well as with other applicable key stakeholders internal and external to the organization. The strategic planning process entails several components which change over time such as market pricing, regulatory uncertainty, and availability of capital. Considering these items and others while factoring in key risks (such as stability of cash flows, market volatility, and market liquidity), a comprehensive, robust, and flexible strategy/plan is developed.

This insurance process involves assessing emerging industry risks in addition to currently known exposures to loss and formulating plans to minimize the impact of an adverse event to the company. Such plans may include risk avoidance (not undertaking a certain activity), risk control (reducing the likelihood or impact of an event), risk transfer (via contract, traditional insurance, or non-traditional insurance methods), or a combination of the aforementioned techniques.

In conjunction with each insurance program renewal, a renewal strategy meeting is held with the applicable insurance broker. The purpose of these meetings is to set both near-term and long-term objectives for the specific insurance program in question. Topics typically addressed include, but are not limited to:

1. Current and projected industry trends (specific to the insurance coverage in question and the insurance market as a whole)
 - a. Pricing
 - b. Coverage enhancements/restrictions
 - c. New carriers
 - d. Large insurable events impacting the industry
2. Peer and industry benchmarking
3. Evaluation of known best practices
4. Design of a renewal strategy

Organizational Structure and Responsibilities:

The Risk Management function falls under the control of the CFO. While not a direct reporting relationship, frequent communication and consultation occurs with AES Corporate Risk Management Oversight Committee and the US SBU RMC.

1. Risk Management is responsible for (1) ensuring proper identification, analysis, and reporting of risks most critical to the organization, (2) ensuring compliance with the risk policy, (3) enforcing risk governance, and (4) promoting an active risk culture. This is accomplished through:
 - a. Routine and adhoc risk reporting
 - b. Monthly RMC meetings
 - c. Quarterly risk updates to Corporate Risk Oversight Committee
 - d. Annual risk diagnostic survey and quarterly heat map update
 - e. Interaction with commercial team members and other key stakeholders regarding the company's evolving risk profile, drivers of change, and preparation of a market risk management strategy
 - f. Annual meeting with Internal Audit regarding upcoming year audit plans
2. Insurance Risk Management is responsible for protecting the company's assets from loss while simultaneously ensuring, to the greatest extent possible, a predictable level of cash flow and expenses. This is accomplished through:
 - a. Continual evaluation of insurable risks facing the organization
 - b. The purchase of traditional insurance
 - c. Diligent management of DPL's captive insurance company, Miami Valley Insurance Company
 - d. Contractual risk management/risk transfer
 - e. Advocating strong loss control processes (specific to both liability and property exposures)
 - f. Development of programs geared towards reducing the exposure to loss

The organizational chart for Risk Management is included as Risk Management – Exhibit 1.

Decision-Making and Control:

The decision-making process is governed by the risk policy which authorizes traders, products, and limits approved by the RMC. For any items not defined within or outside the risk policy, the RMC or other predetermined approver must authorize. Any decision requiring a RMC vote must receive majority approval, with certain members of the RMC having veto rights.

The operations of the Miami Valley Insurance Company are subject to the applicable State of Vermont captive statutes and are further governed by the Miami Valley Insurance Company Board of Directors. A business plan is executed in conjunction with the annual board meeting and any deviations from this plan must be approved by the board. To ensure transparency and appropriate pricing (market insurance rates), pricing studies are conducted by an outside actuary in conjunction with each program renewal (currently, excess liability, workers' compensation, and property insurance are written within the captive). Additionally, semi-annual loss reserve studies are completed, again by outside actuaries, to ensure appropriate loss reserving practices. Finally, all financial reports are prepared by an independent auditor and submitted to the State of Vermont for review and approval.

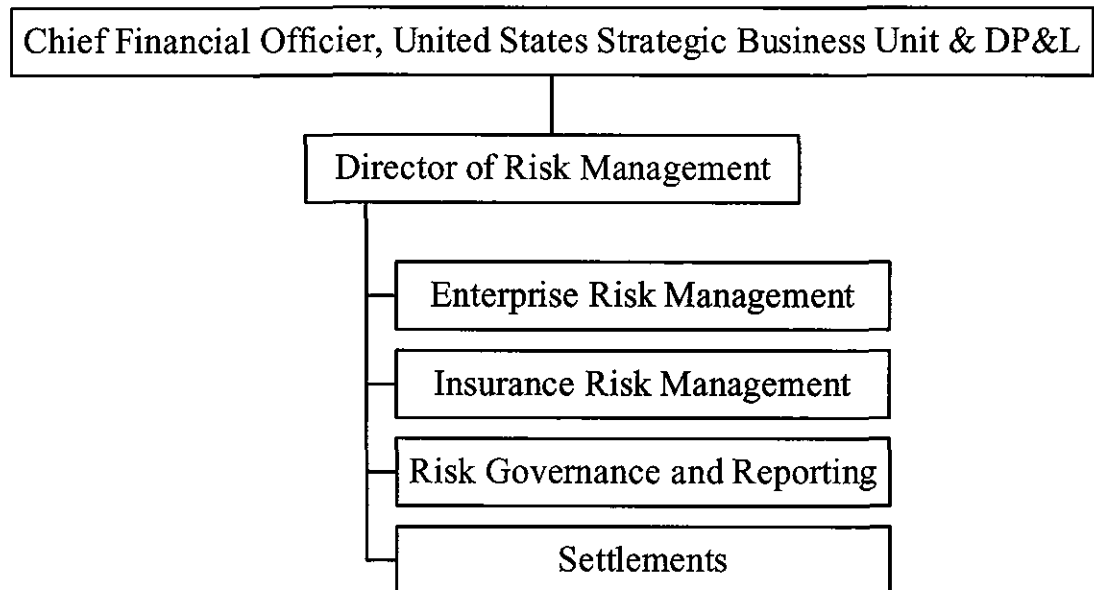
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including: face-to-face meetings, phone calls, conference calls and e-mail. Internal communications on a daily basis includes conversations with Accounting, Supply Chain, Legal, Commercial Operations, Customer Service and AES corporate personnel. These conversations will typically involve insurance procurement, claims and contracts.

External communications are accomplished through a variety of communication channels including: phone calls, meetings, and e-mail. External communication occurs on a less frequent basis and can include, but is not limited to: external auditors, legal counsel, consultants, Miami Valley Insurance Company, claims adjusters, insurance brokers and insurance carriers.

Risk Management – Exhibit 1

Organizational chart for Risk Management



Functional Area:
Tax Department**Policy and Goal Setting:**

DP&L's Tax Department policies have evolved to be responsive to federal, state and local taxing authorities and regulators. DP&L's policies are developed by DP&L's management under the guidance of AES's Management and Board of Directors.

The first priority of all DP&L areas is to ensure the safety of all DP&L employees, contractors and the public. The safety program focuses on getting everyone involved in safety in order to increase safety awareness and create an injury-free workplace. The Tax Department supports these efforts by conducting monthly safety meetings, attending an annual safety awareness day as well as participating in the safety walk program.

The goal setting process for the Tax Department is a joint effort between the AES Chief Tax Officer, CFO and the US SBU Director of Tax. The goals and objectives of the Tax Department are established on an annual basis in support of overall DP&L and AES Corporate goals. Progress toward achieving the annual goals of the Tax Department is reviewed periodically as required.

The goals of the Tax Department are established to support the following objectives:

1. To comply with all applicable federal, state, and local tax laws
2. To ensure filing of all returns and payments on a timely basis
3. To assure that DP&L's tax accounting practices are in accordance with the respective regulatory agencies' requirements
4. To support DP&L's position in regulatory initiatives
5. To participate in the development of tax legislation
6. To provide tax assistance as may be requested by others in the organization

Strategic and Long-Range Planning:

AES's Management and the Board of Directors have the primary responsibility for establishing DP&L's business plan. The Tax Department sets general and specific goals to support the business plan established by senior management.

The Tax Department participates in the corporate planning process through the recurring budgeting process and also by providing expert advice on the tax implications of various commercial decisions. Furthermore, the Tax Department pursues efficient tax positions built upon sound commercial practices within the boundaries of any and all applicable laws and regulations.

Organizational Structure and Responsibilities:

The Tax Department is headed by the US SBU Director of Tax who reports directly to the US SBU CFO and indirectly to the AES Senior Director of US Tax Reporting and Corporate Planning. The Department is currently divided into three principle functional areas: (1) Tax accounting and regulatory compliance; (2) Tax center of excellence (including federal income tax, state and local income and franchise tax, property tax, sales and use tax, and fixed assets); and (3) Planning and controversies. The day-to-day operations of these areas report directly to the US SBU Director of Tax.

It is the Tax Department's responsibility to prepare, assemble, review and file certain tax returns and reports for filing along with forecasting, verifying and remitting payments of such taxes. Furthermore the Tax Department establishes and records all accounting entries necessary for the proper determination of tax liabilities and expenses in accordance with statutory and regulatory requirements.

The specific responsibilities of the Tax Department include the following:

1. Prepare and file, on a timely basis, appropriate federal, state, and local, annual, quarterly, and monthly income and non-income tax returns
2. Forecast, verify, request, and remit payments of taxes
3. Develop and maintain necessary supporting documentation for such tax returns and computations
4. Conduct tax research, including the review of current statutes, regulations, tax decisions, rulings, judicial authority, and analyses of proposed legislation to determine their effect on the operations of DP&L and AES
5. Communicate tax research findings to appropriate levels of the Company and assist in formulating appropriate strategies to achieve reasonable and responsible outcomes
6. Provide DP&L's and AES' responses to inquiries made by various tax authorities upon audit
7. Defense of DP&L's and AES' tax positions by filings appeals and protests, as necessary
8. Prepare tax accounting journal entries

The organizational chart for the Tax Department is included as Tax Department - Exhibit 1.

Decision-Making and Control:

Tax Department decision-making and control is achieved by individuals making decisions within their given scope of authority in support of DP&L's and AES' overall mission and in accordance with applicable policies and procedures. Decisions are raised to the proper level of authority as required by such policies. Overall responsibility for all decisions belongs to the US SBU CFO, the AES Chief Tax Officer, and the US SBU Director of Tax.

Certain guiding principles on taxation, statutory guidance and adequate internal control support the overall decision-making processes and control environment of the function. Such decision-making and controls principally relate to the proper measurement, timing, and reporting of tax data in returns as well as in financial statements.

General knowledge needed to make appropriate tax and accounting decisions is obtained through research of relevant guidance. Accounting research may be required as a result of changes required by the Financial Accounting Standards Board, federal or state regulatory commissions, or new financial, economic, or commercial circumstances. Additionally, new legislation, court decisions, and changes in tax statutes or regulations may require research.

In addition to internal review and controls covering tax and accounting changes as well as documentation of significant tax positions, compliance related to accounting is attested to by internal and/or external auditors. Ultimately, compliance with tax laws may be verified through periodic audits conducted by representatives of various taxing authorities.

Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including, but not limited to: face to face meetings, video conferences, teleconferences, and email. Such communication occurs among personnel within the Tax Department discussing routine and special projects as well as on a cross-functional basis in order to provide assistance in tax-related matters and to stay informed of commercial activities.

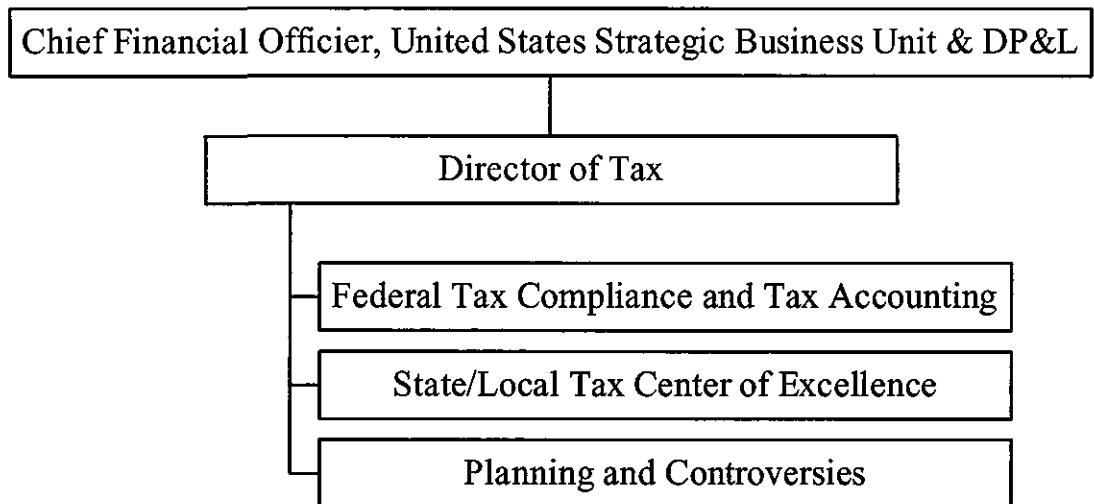
Periodic staff meetings are held by the AES Chief Tax Officer as well as by the US SBU Director of Tax. These meetings provide a forum for discussing commercial events that affect tax operations, updates on projects, as well as discussions regarding priorities and practices. Furthermore, Tax Department personnel participate in periodic CFO staff meetings, allowing for the communication and identification of tax-related issues.

On an as-needed basis, Tax Department personnel may seek counsel from external tax and legal experts regarding tax and accounting issues which may impact DP&L or AES. Tax Department personnel must also liaise with external auditors during their review of the financial statements and regulatory reports as they pertain to tax matters recorded or disclosed.

The main form of external communication with taxing authorities is in the form of the required periodic tax filings and or returns. Additionally, outside contacts are made regularly, in both written and oral form, with such taxing authorities when audits or controversies are encountered.

Tax Department – Exhibit 1

Organizational Chart for Tax Department



Functional Area:**Treasury****SFR Reference****(B)(9)(b)(i) Cash management****Policy and Goal Setting:**

The financial functions of DP&L are primarily provided by AES US Services, LLC (“US Services”). As established in the Services Agreement dated December 2013 US Services is responsible for the provision of all financial functions of DP&L.

All of the policies governing the financial functions at US Services are ultimately the responsibility of the CFO, who is required to protect all the financial assets and manage all of the financial resources of each signatory under the Services Agreement, including DP&L.

US Services’ financial policies are developed by the leaders of each respective and relevant functional area of the Company in conjunction with AES, and each financial policy is designed to mirror the policies of AES or compliment them, taking into account distinct business issues and the regulatory framework of Ohio or other relevant jurisdictions. The policies are then adopted by the US Services Management team and may be, but are not in all circumstances, subject to approval by DP&L or other relevant businesses’ Board of Directors. All parties involved in the development and implementation of the policies are equally responsible to ensure that these policies, which govern DP&L business activities, meet or exceed the requirements set forth by all of DP&L’s regulatory entities.

Financial policies that are specifically related to the Treasury, and which govern among other things how financial assets are collected, disbursed, concentrated, invested and funded are developed by the US Services Treasurer and CFO before being subject to the approval process described above. The following activities are some, but not all, of the financial activities of DP&L that are governed by the Treasury policies of US Services:

1. Open and close bank accounts
2. Make short term cash investments
3. Electronic funds transfer, check signing and general disbursements of cash
4. Grant liens
5. Borrow funds through internal or external sources
6. Set expenditure approval authorities
7. Administer commercial cards

The Treasury Department has been designed, staffed and structured to support and achieve the business strategy of DP&L. Broadly speaking, the Treasury’s ultimate goal is to maximize liquidity and mitigate operational, financial and reputational risk. More specifically and as it relates to DP&L, Treasury is focused, among other things, on the following objectives:

1. Optimize capital structure (managing to a target capitalization level and appropriately balancing debt maturity profiles with cost of debt alternatives)
2. Optimize liquidity profile (maintaining adequate working capital and liquidity backstops to support collateral calls, unexpected events and enhance overall credit profile)
3. Efficiently invest/manage financial assets (allocating capital in the most productive manner whether it be through reinvestment, debt repayment, distribution to DPL Inc, or short term investing)
4. Ensure Treasury payments are made on time and in an efficient manner
5. Establish and maintain actionable reporting and strong internal control environments related to the key Treasury activities (including receipt, investing and disbursements of cash)
6. Work with credit rating agencies to communicate the DP&L business strategy, and to support and encourage appropriate credit ratings

Strategic and Long-Range Planning:

Strategic and long-range planning in the Treasury Department concentrates on the efficient and effective management of financial assets. On a day to day basis Treasury utilizes bank statements and online portals to position cash and verify the amount of overall liquidity DP&L has available to it. Treasury uses this actual data along with short term (balance of year) and long-term (multiple years) cash forecasts to manage both current and future liquidity needs of DP&L. These cash forecasts estimate among other things:

1. The timing and levels of expected collections and disbursements
2. The size, timing and tenor of short term credit requirements to bridge working capital deficits
3. The amount of excess cash available for reinvestment, short term investing, debt repayments or dividends
4. Capital adequacy in the event of unforeseen or unplanned events such as large margin calls, storms or other major outages
5. The long-term financing or refinancing needs of the businesses, to support growth or maintenance capital expenditures
6. The size and timing of contributions to the relevant pension plans

Cash positions are updated daily and are complimented with new cash forecasts no less than on a monthly basis. This information combined with corporate policy, market information, and other company specific information is used to ensure adequate liquidity over the next 90 day period, and optimal liquidity positions over the long term. All long-term cash forecasts and strategic initiatives embedded in these forecasts are reviewed and approved by the CFO.

Treasury through its Corporate Finance team also provides management oversight of the assets in DP&L's defined benefit plans, 401(k) plans, and other post-retirement plans. Corporate Finance enlists the support of Human Resources and external service providers in striving to

effectively meet the goals and objectives of these retirement plans, as well as compliance with appropriate governmental entities.

Organizational Structure and Responsibilities:

Treasury is divided into three areas: Corporate Finance, Credit and Compliance, and Treasury Operations. The leaders of these areas all report directly to the Treasurer, who in turn reports to the CFO. The organizational chart of the Treasury team is attached as Treasury - Exhibit 1.

The responsibilities of each of these areas are as follows:

1. Corporate Finance
 - a. *Financing*: Corporate Finance is primarily responsible for the development and execution of the short and long-term financing plans of the company in accordance with its financial objectives such as obtaining a target capital structure, financing growth and maintaining target credit ratings. Corporate Finance maintains an active dialogue with commercial and investment banks to keep abreast of current financing markets and opportunities/alternatives to raise capital in a cost effective manner. Once a transaction is in “execution” Corporate Finance will lead a financing team consisting of several outside parties including underwriters, placement agents, advisors, arrangers, banks, legal advisors, credit rating agencies, trustees, administrative agents, auditors and other parties necessary to finalize a transaction.
 - b. *Credit Rating Agencies*: Corporate Finance also serves as the primary conduit between the credit rating agencies and the management of the companies. In this role Corporate Finance leads the annual review process, the subsequent question and answer sessions, provides regular updates to the rating agencies of key developments, and reviews ratings releases prior to publication.
 - c. *Pension & Retirement Services*: Finally, Corporate Finance is also responsible for the oversight of the management and administration of the company’s retirement plans. This includes analyzing and sending contributions to the various plans, calculating and funding benefit payments, monitoring and analyzing the advice of investment consultants, researching and performing due diligence of possible investment selections and tracking fund manager performance against benchmarks, and maintaining compliance with Employee Retirement Income Security Act and other governmental entities. Performance is reported periodically to the Pension and Benefits Committee of the Board of Directors and annually to the Board of Directors.
2. Credit and Compliance
 - a. *Credit*: the primary responsibilities of credit include (i) evaluating credit risk and making decisions concerning credit limits with counterparties, (ii)

- determining acceptable levels of risk, terms of payment and credit assurances required in certain contracts with certain vendors, and (iii) tracking and managing collateral exposure created through hedging agreements and other commercial contracts. In addition, the credit function is responsible for setting and ensuring compliance with a corporate credit policy, obtaining security interests or credit assurances where necessary, establishing terms of credit assurances and initiating legal or other recovery actions against vendors who are delinquent.
- b. *Compliance:* Compliance is responsible for administering loans, tracking compliance with different financing documents (credit agreements, indentures, note purchase agreements, reimbursement obligations, etc.), measuring financial covenants, and acting as cash managers for the respective businesses. As cash managers, Compliance uses the cash balances provided by Treasury Operations and relevant cash data from different parts of the organization to develop short term cash flow forecasts. With these forecasts, along with the long-term forecasts provided by the Financial Planning & Analysis Group the cash manager will assess liquidity and instruct Treasury Operations how excess cash should be utilized (reinvestment, Short term investing, debt repayment, dividends, etc.). Conversely when it is necessary to borrow on the company's revolving credit facility, compliance personnel will notify the relevant administrative agents and provide the requisite certification in order to gain access to the funds.
3. Treasury Operations
 - a. Treasury operations provides daily cash positioning, transaction recording, initiation and execution of electronic funds transfers, and short-term investing and borrowing of corporate funds, as appropriate. Treasury Operations provides various cash position reports and analyses to the Treasury Operations leader, and as necessary to the Treasurer, depicting the daily cash activity and illustrating the Company's general cash/liquidity position. Treasury Operations personnel are also responsible for opening and closing bank accounts, optimizing bank account structures and developing and maintaining commercial banking relationships to support the company's back office banking needs. When the company has excess cash, Treasury Operations works with Compliance personnel to evaluate different investment opportunities in line with the company's investment policies and then makes those investments.

Decision-Making and Control:

Ultimate decision-making authority for day-to-day, normal course of business activities resides with the Treasurer, whereby the Treasurer delegates decision-making authority to each functional leader as appropriate. Long-term cash management forecasts, extraordinary expenditures or

approval to proceed with unplanned/unbudgeted initiatives within Treasury could elevate to the CFO depending on the scope and financial impact. Decisions related to formally binding DP&L, approving expenditures and other similar types of activities are governed by policies and procedures of US Services.

Performance against the objectives of the Treasury are monitored and reported on a continuous basis. Annual performance objectives for each area within Treasury are established once a year and are formally measured in the middle and end of that year. In addition, Treasury continuously tracks and reports on KPIs metrics including; current and forecasted cash balances, key credit statistics and/or financial covenants, debt repayment targets, new financing levels and prices, and working capital statistics. Monthly goals are established during each budget year for each of these metrics and are tracked monthly as part of the management performance report. Continuous monitoring helps to ensure that objectives stay on track and are achievable.

It should be noted that objectives and goals are dynamic. As high priority issues arise, objectives are recalibrated to ensure the Treasury is working on the projects that are in the best interest of customers, shareholders, and the Company.

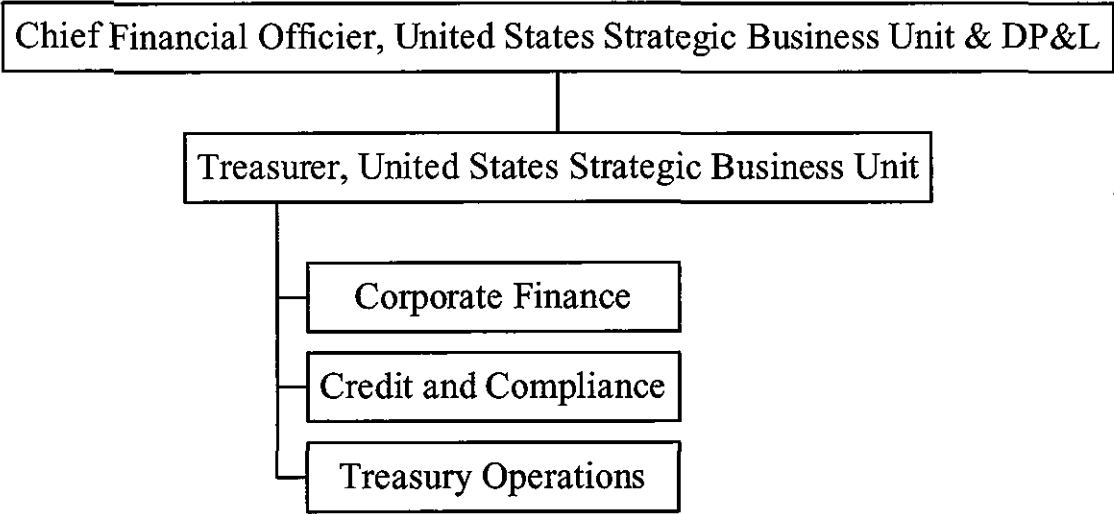
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels (formal and informal) including: in-person/telepresence meetings for staff and leadership, phone calls, conference calls and e-mail. Messages communicated include policies and decisions of management, discussion of work assignments and priorities, upcoming events and other items of interest to Treasury personnel. An open forum exists for all employees to discuss problems, concerns and suggestions through these communication channels as appropriate.

External communications are ongoing with banks (commercial and investment), credit rating agencies, benefit plan consultants and managers, trustees, and others in order to conduct business on behalf of and for the benefit of DP&L.

Treasury – Exhibit 1

Organizational chart for Treasury



THE DAYTON POWER & LIGHT COMPANY

Case No. 15-1830-EL-AIR

Supplemental Information (C)(1)

Requirement:

Provide the most recent federal regulatory agency's (FERC) audit report.

Response:

Please see attached most recent FERC audit report.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

In Reply Refer To:
Office of Enforcement
Docket No. PA12-6-000
June 6, 2013

AES Corporation
Attention: Mr. Brian Miller
Executive Vice President and General Counsel
4300 Wilson Blvd.
Arlington, VA 22203-4168

Dear Mr. Miller:

1. The Division of Audits within the Office of Enforcement has completed an audit of AES Corporation (AES) and its subsidiary companies (collectively, Companies). The audit evaluated the Companies' compliance with the conditions established in the Commission's Orders Authorizing Merger and Disposition of Jurisdictional Facilities issued March 9, 2010¹ and Disposition of Jurisdictional Facilities issued November 15, 2011.² The enclosed audit report contains no audit findings or recommendations.
2. On May 10, 2013, you notified us that the Companies agreed with the audit report. A copy of your response is attached to this report.
3. The Commission delegated the authority to act on this matter to the Director of OE under 18 C.F.R. § 375.311 (j) (2012). This letter order constitutes final agency action. You may file a request for rehearing with the Commission within 30 days of the date of this order under 18 C.F.R. § 385.713 (2012).
4. This letter order is without prejudice to the Commission's right to require hereafter any adjustments it may consider proper from additional information that may come to its attention. In addition, any instance of non-compliance not addressed herein or that may occur in the future may also be subject to investigation and appropriate remedies.

¹ AEE 2, L.L.C., 130 FERC ¶ 62,205 (2010).

² The AES Corporation, 137 FERC ¶ 61,122 (2011).

AES Corporation

Docket No. PA12-6-000

5. I appreciate the courtesies extended to the auditors. If you have any questions, please contact Mr. Bryan K. Craig, Director and Chief Accountant, Division of Audits at (202) 502-8741.

Sincerely,

Norman C. Bay
Director
Office of Enforcement

Enclosure



Federal Energy Regulatory Commission

Audit of AES Corporation and its Subsidiaries for Compliance with Conditions in the Commission's Orders Authorizing Merger and Disposition of Jurisdictional Facilities

Docket No. PA12-6-000
June 6, 2013

Office of Enforcement
Division of Audits

TABLE OF CONTENTS

| | |
|--|-----------|
| I. Executive Summary | 1 |
| A. Overview..... | 1 |
| B. AES, CIC and DPL..... | 1 |
| C. Audit Conclusion | 2 |
| II. Background..... | 3 |
| A. AES/CIC Transaction | 3 |
| B. AES/DPL Transaction | 5 |
| III. Introduction | 7 |
| A. Objectives | 7 |
| B. Scope and Methodology | 7 |
| Appendix: Audit Report Comments | 11 |

I. Executive Summary

A. Overview

The Division of Audits within the Office of Enforcement has completed the audit of AES Corporation (AES) and its subsidiary companies (collectively, Companies) that commenced November 21, 2011. The audit evaluated the Companies' compliance with conditions established in the Commission's Orders Authorizing Merger and Disposition of Jurisdictional Facilities issued March 9, 2010¹ and Disposition of Jurisdictional Facilities issued November 15, 2011.² The audit covered March 9, 2010 through August 31, 2012.

B. AES, CIC and DPL

The AES merger and disposition of jurisdictional facilities involved two separate transactions among different companies. In the AES and China Investment Corporation (CIC) transaction, the Commission authorized Terrific Investment Corporation (Terrific), a wholly owned subsidiary of CIC to acquire a 15 percent ownership interest in AES, the parent company of the AES applicants.³ In the AES and DPL, Inc. (DP&L) transaction, the Commission authorized AES to acquire 100 percent of DPL and its subsidiaries. The corporate structure and affiliations of the Companies at the time of application are described below.

AES Corporation

AES is a global power company that owns electric generation, transmission, and distribution facilities in 29 countries. AES indirectly owns 13,000 MW of generation in the United States through AES applicants (each is a public utility with market-based rate authority), qualifying facilities under the Public Utility Regulatory Policies Act of 1978 (PURPA),⁴ and other competitive wholesale generation companies. Also, one AES subsidiary is Indianapolis Power & Light Company (IPL) a traditional, vertically

¹ AEE 2, L.L.C., 130 FERC ¶ 62,205 (2010).

² The AES Corporation, 137 FERC ¶ 61,122 (2011).

³ AES applicants are AEE 2, L.L.C., AES Alamitos, L.L.C.; AES Armenia Mountain Wind, LLC; AES Energy Storage, LLC; AES Creative Resources, L.P.; AES Eastern Energy, L.P.; AES Ironwood, L.L.C.; AES Red Oak, L.L.C.; AES Huntington Beach, L.L.C.; AES Redondo Beach, L.L.C.; AES Placerita, Inc.; Condon Wind Power, LLC; Lake Benton Power Partners, LLC; Mountain View Power Partners, LLC; Storm Lake Power Partners II, LLC; and Indianapolis Power & Light Company.

⁴ 16 U.S.C. § 824a-3 (2012).

AES Corporation

Docket No. PA12-6-000

integrated utility. IPL has no captive or bundled wholesale customers, and has market-based rate authority to make wholesale sales of electricity.

China Investment Corporation

CIC is an investment company headquartered in Beijing whose sole shareholder is the State Council of the People's Republic of China (PRC). CIC invests in private equity and other funds, which may in turn have some level of investment directly or indirectly in energy assets. But such CIC investments are in the form of passive, limited partnership interests that do not give CIC the ability to influence or control day-to-day operations and investment activities of those funds or energy assets. Terrific, a company incorporated under PRC law, is a wholly owned subsidiary of CIC that was formed to implement investment transactions like the one involving AES and CIC. CIC also has less than a 10 percent common stock passive ownership interest in Morgan Stanley and a 10 percent passive interest in the form of nonvoting common stock in the Blackstone Group.

DPL, Inc.

DPL is a diversified regional energy company based in Dayton, OH. DPL indirectly owns and operates some 3,929 MW of generating capacity in the PJM market. DPL through its principal subsidiaries Dayton Power and Light (DP&L), DPL Energy, LLC (DPLE), and DPL Energy Resources, Inc. (DPLER) generates and sells wholesale electricity and distributes and sells retail electricity to customers in west central Ohio. As to these affiliates, DP&L relinquished operational control of its bulk-power transmission facilities to PJM, conducts wholesale power activities through its Commission-approved market-based rate authority, and distributes power to retail customers under Ohio's retail choice program. DPLE owns and operates merchant generation facilities within the PJM market and has market-based rate authority to sell wholesale electricity. DPLER is an active competitive retail supplier in Ohio and nonactive alternative retail supplier in the states of Illinois, Michigan, and Pennsylvania.

C. Audit Conclusion

The audit did not result in any findings or recommendations that require the Companies to take corrective action at this time. Audit staff based its conclusion on the review of publicly available documents, materials provided in response to data requests, interviews with employees, and independent analysis.

II. Background

A. AES/CIC Transaction

Application Requesting Disposition of Jurisdictional Facilities

On January 11, 2010, as supplemented on February 25, 2010, AES and CIC filed an application under FPA section 203(a)(1)⁵ requesting authorization for Terrific to acquire a 15 percent ownership interest in AES, the parent company of the AES applicants.⁶ CIC made it clear in the application that it does not consider itself to be a holding company subject to FPA section 203(a)(2). As a result, AES and CIC requested transaction approval under FPA section 203(a)(1).⁷

In this transaction and under a stock purchase agreement dated November 6, 2009, AES proposed to issue and sell to Terrific 125,468,788 shares of AES common stock on a fully diluted basis for \$1.58 billion (\$12.60 per share). The jurisdictional facilities involved in this transaction consisted of AES' interconnection facilities, market-based rate schedules, power sales contracts, and various books and records, and IPL's transmission facilities and tariffs.

Commission Order Authorizing Disposition of Jurisdictional Facilities

On March 9, 2010, the Commission approved the application by issuing an Order Authorizing Disposition of Jurisdictional Facilities.⁸ The Commission authorized the proposed transaction and imposed these conditions upon the Companies:

- Inform the Commission within 30 days of any change in circumstances that would differ from the facts it relied upon to approve the transaction.
- Notify the Commission within 10 days of disposing jurisdictional facilities.
- Make all appropriate filings under FPA section 205 as necessary to implement the proposed transaction.

⁵ 16 U.S.C. § 824b (2012).

⁶ AEE 2, L.L.C., Application for Authorization Under Section 203 of the Federal Power Act and Request for Expedited Action, Docket No. EC10-37-000 (filed January 11, 2010).

⁷ Id. at 16.

⁸ See *supra* note 1.

- Make recertification filings under 18 C.F.R. § 292.207 if the transaction results in a change in status or upstream ownership in affiliated qualifying facilities.
- Comply with Order No. 652 requirements to ensure necessary filings under FPA section 205 are made to implement the transaction. Order No. 652 requires sellers with market-based rate authority to timely report any change in status that departs from characteristics the Commission relied upon in granting market-based rate authority.
- Information and systems in this transaction connected to the bulk-power system may be subject to cyber security standards under FPA section 215, regardless of the physical location of affiliates, investors, information databases and operating systems involved. A public utility must take measures to deny access to information, equipment, and software connected to the bulk-power system to its affiliates, employees, and investors not authorized to have access to the information and systems. Mechanisms to deny access must comply with all applicable reliability and cyber security standards.

Besides these conditions, AES and CIC made certain assertions that the Commission relied upon to approve the transaction.

- CIC owns and will continue to own less than a 10 percent common stock interest in Morgan Stanley. CIC is a passive investor with no role in Morgan Stanley's management. As a passive investor, CIC also holds a 10 percent interest in the Blackstone Group in the form of nonvoting common stock units.
- CIC through Terrific indirectly will own about 15 percent of AES common stock upon consummation of the transaction. As long as Terrific holds 5 percent or more of AES' common stock, Terrific can nominate for election to AES' Board one representative at each annual meeting. If elected, this official will have no special powers or rights in Board decisions. Terrific, CIC, and affiliates are subject to stand-still and lockup restrictions that limit their ability to buy or sell voting securities of AES.

B. AES/DPL Transaction

Application Requesting Merger and Disposition of Jurisdictional Facilities

On May 18, 2011, AES, DPL, and DPL's public utility subsidiaries DP&L and DP&L filed a joint application under FPA sections 203(a)(1) and 203(a)(2),⁹ requesting Commission authorization for AES to acquire 100 percent of DPL and its subsidiaries.¹⁰ In the proposed transaction, AES would acquire DPL under a stock-for-cash exchange where DPL shareholders receive \$30 per share of common stock.

The Agreement and Plan of Merger, dated April 19, 2011 contained the terms and conditions for the proposed transaction, by and among DPL, AES, and Dolphin Sub.¹¹ Under the agreement, Dolphin Sub would merge with and into DPL. As a result of the merger, Dolphin Sub ceased to exist, DPL would become a wholly owned direct subsidiary of AES, and DP&L and DP&L become indirect subsidiaries. After consummation of the proposed transaction, AES would hold all DPL's outstanding shares of common stock, and DPL stock would no longer be publicly traded.

Commission Order Authorizing Merger and Disposition of Jurisdictional Facilities

On November 15, 2011, the Commission approved the application by issuing an Order Authorizing Merger and Disposition of Jurisdictional Facilities.¹² The Commission authorized the proposed transaction and imposed these conditions upon the Companies:

- Inform the Commission within 30 days of any change in circumstances that would differ from the facts it relied upon in granting the application.
- Notify the Commission within 10 days of disposing jurisdictional facilities.
- Make all appropriate filings under FPA section 205 as necessary to implement the proposed transaction.
- Make a compliance filing within 30 days of order issuance to correct the typographical error in Exhibit M of the application.

⁹ 16 U.S.C. § 824b.

¹⁰ The AES Corporation, Application for Authorization of Disposition of Jurisdictional Assets and Merger under sections 203(a)(1) and 203(a)(2) of the Federal Power Act, Docket No. EC11-81-000 (filed May 18, 2011).

¹¹ Dolphin Sub, Inc., an Ohio corporation, is a wholly owned subsidiary of AES formed on April 8, 2011 and was created solely for effecting the merger transaction.

¹² See *supra* note 2.

- File accounting entries within six months of consummating the proposed transactions involving entities subject to the Commission's Uniform System of Accounts that record any aspect of the proposed transaction in its accounts. An entity recording accounting entries after the six-month period has to file these entries within 60 days of recording them.
- Make a compliance filing to recover transaction-related costs through wholesale power or transmission rates. The filing must detail how the entity seeking recovery satisfies the hold-harmless requirements, identify transaction-related costs the entity seeks to recover, and demonstrate how savings produced from the merger and disposition of jurisdictional facilities equals or exceeds transaction-related costs.
- Information and/or systems in this transaction connected to the bulk-power system may be subject to cyber security standards under FPA section 215, regardless of the physical location of the affiliates, investors, information databases, and operating systems involved. A public utility must take measures to deny access to information, equipment, and software connected to the bulk-power system to affiliates, employees, and investors not authorized to have access to the information and systems. Mechanisms to deny access must comply with all applicable reliability and cyber security standards.

Besides these conditions, AES and DPL asserted the proposed transaction has no adverse effect on wholesale cost-based rates. To provide further assurance, the Companies committed to hold transmission and wholesale requirement customers harmless for five years from all transaction-related costs, not only costs related to consummating the proposed transaction.

III. Introduction

A. Objectives

The audit evaluated whether the Companies complied with conditions in the Commission's Orders Authorizing Merger and Disposition of Jurisdictional Facilities issued March 9, 2010¹³ and Disposition of Jurisdictional Facilities issued November 15, 2011.¹⁴ The audit covered March 9, 2010 through August 31, 2012.

B. Scope and Methodology

Audit staff performed specific steps to facilitate its evaluation of the Companies' compliance with audit scope areas. Specifically, audit staff:

- Reviewed publicly available materials, including filings and orders, and other relevant information in the Commission's eLibrary records system and available on public web sites.
- Identified standards and criteria to evaluate compliance with the conditions embodied in the Commission's order. These standards and criteria included rules, regulations, and statutes governing the disposition of jurisdictional facilities transaction.
- Issued data requests to gather information needed to evaluate compliance with conditions outlined in the Commission's Order. Audit staff used this information as its underlying support for compliance testing and evaluating.
- Conducted teleconferences with company employees to discuss administrative and technical matters relevant to the audit scope. These calls served as the primary communication channel with employees throughout the audit. Administrative matters pertained to audit process and data requests, while technical matters pertained to specific areas relevant to the audit scope.

Audit staff performed specific actions to evaluate compliance with the conditions embodied in the Commission's order approving the disposition of jurisdictional facilities and other applicable Commission regulations associated with the AES and CIC transaction. Specifically, audit staff:

¹³ See supra note 1.

¹⁴ See supra note 2.

- Reviewed regulatory activities to confirm required filings were made upon consummating and implementing the transaction with the Commission. Also, whether the Companies filed to request recovery of transaction-related costs before satisfying the hold-harmless requirements.
- Reviewed information in the disposition of jurisdictional facilities application, corporate organizational charts, and other sources to identify affiliates with market-based rate authority and changes in ownership or control of generation or transmission facilities since filing the application. Audit staff used this information to determine whether departures from circumstances the Commission relied upon to approve the transaction occurred and for granting market-based rate authority. For any changes, audit staff confirmed the Companies made appropriate filings with the Commission.
- Examined the Companies' disposition of jurisdictional facility application, generation resource portfolio, and other sources to identify change in status or upstream ownership for qualifying facilities. Audit staff used this information to determine whether the Companies needed to file with the Commission for certification or recertification of qualifying facilities with the Commission.
- Reviewed applicability of reliability and cyber security standards, and mechanisms the Companies used to deny access to information and systems connected to the Bulk-Power System. Audit staff limited its review to critical assets and critical cyber assets.
- Reviewed generation and transmission facilities AES and CIC owned and controlled to ensure the accuracy of assertions relating to vertical and horizontal market power in their application.
- Examined security filings and trade confirmations to validate CIC accurately reflected its ownership interest in AES, Morgan Stanley, and Blackstone in the application, and those interests remained below levels of controlling interest or of limited voting power to preclude them from having the ability to influence management's decision making at these companies.
- Reviewed CIC and its affiliate's positions, powers, and voting rights on AES' Board of Directors to ensure decision making control did not exist, and the positions held were within the confines of its application.
- Reviewed organizational structure in periods subsequent to the merger to identify new associate companies and determine whether these companies

imposed concerns related to cross subsidization and the pledge or encumbrance of utility assets for the benefit of an associate company.

The AES and DPL transaction contained many of the same conditions as the previous transaction involving AES and CIC. The most significant difference in the AES and DPL transaction was the assertion pertaining to the effect on rates. The Companies committed not to include merger-related costs in their transmission revenue requirements or in any wholesale requirements rates, except to the extent they could demonstrate that merger-related savings are equal to or more than the transaction-related costs included in the rate filing for a five-year period. The Commission conditioned this by requiring the Companies to make a compliance filing if they planned to recover transaction-related costs through wholesale power or transmission rates before the five year period. To evaluate this assertion audit staff:

- Reviewed the Companies' procedures, processes, and controls implemented to track transaction-related costs and prevent premature recovery of these costs from transmission and wholesale requirement customers.
- Examined the accumulation of transaction-related costs on the holding company's books and the underlying accounting for these costs.
- Examined franchised public utility companies with captive customers to determine whether the holding company assigned any transaction-related costs to them.
- Evaluated rate mechanisms and identified changes in fixed cost of service rates since the transaction consummated, to determine whether the Companies recovered transaction-related costs before the five-year period, absent making a filing with the Commission.
- Held discussions with the Companies' accounting and ratemaking employees to determine whether they plan to file to recover transaction-related costs before the five-year period.
- Reviewed organizational structure in periods after the merger to identify new associated companies and determine whether these companies imposed concerns related to cross-subsidization and the pledge or encumbrance of utility assets for the benefit of an associate company.

Besides these compliance tests, audit staff conducted a limited review of the Companies' regulatory compliance program relative to the audit objective and prior Commission policy statements on compliance focusing on: (1) the role of senior

AES Corporation

Docket No. PA12-6-000

management in fostering compliance; (2) effective preventive measures to ensure compliance; (3) prompt detection, cessation, and reporting of violations; and (4) remediation efforts.

AES Corporation

Docket No. PA12-6-000

Appendix: Audit Report Comments

May 10, 2013

Mr. Bryan Craig
Director and Chief Accountant
Division of Audits
Office of Enforcement
Federal Energy Regulatory Commission
888 First Street, N.E., room 5K-13
Washington, DC 20426

Re: Office of Enforcement
Docket No. PA12-6-000

Dear Mr. Craig:

The AES Corporation has received your draft audit report dated May 6, 2013 in connection with the above-referenced docket number. We have no comments to the draft audit report. We appreciate the time, effort and constructive assistance from FERC in working with AES throughout the audit process. If you have any questions, please do not hesitate to call Paul Freedman at (703) 682-1159 or me at (703) 682-6427.

Very truly yours,

Brian A. Miller
Executive Vice President, Secretary and
General Counsel

The AES Corporation

Document Content(s)

PA12-6-000.DOC.....1-15

THE DAYTON POWER & LIGHT COMPANY

Case No. 15-1830-EL-AIR

Supplemental Information (C)(2)

Requirement:

Provide prospectuses of current stock and/or bond offering of the applicant, and/or of parent company if applicant is a wholly owned subsidiary. In the event there are no current offerings, then provide the most recent offerings.

Response:

Please see attached the most recent offering.

OFFERING MEMORANDUM

\$445,000,000



The Dayton Power and Light Company
FIRST MORTGAGE BONDS
1.875% SERIES DUE 2016

Interest payable March 15 and September 15

We are offering \$445,000,000 of our First Mortgage Bonds, 1.875% Series Due 2016 (the "Bonds"). The Bonds will mature on September 15, 2016, unless redeemed prior to that date. The first interest payment on the Bonds will be made on March 15, 2014. The Bonds will be issued only in denominations of \$1,000 and integral multiples of \$1,000. We may redeem the Bonds prior to maturity, in whole or in part, at our option at any time or from time to time, at the make-whole redemption price described in this offering memorandum. See "Description of the Bonds—Optional Redemption."

The Bonds will be our senior secured obligations that will be secured by and under our existing First and Refunding Mortgage, dated as of October 1, 1935, between us and The Bank of New York Mellon, as trustee, as amended (the "Mortgage"). See "Description of the Bonds—Priority and Security." The Bonds will rank equally in right of payment with our other existing or future First Mortgage Bonds issued under the Mortgage. As of June 30, 2013, we had approximately \$884.4 million aggregate principal amount of First Mortgage Bonds outstanding. We intend to use the net proceeds from this offering and cash on hand to repay at maturity \$470.0 million aggregate principal amount of our First Mortgage Bonds, 5.125% Series Due 2013.

We will agree pursuant to a registration rights agreement to file an exchange offer registration statement or, under certain circumstances, a shelf registration statement with respect to the Bonds. See "Exchange Offer; Registration Rights."

Investing in the Bonds involves risks. See "Risk Factors" beginning on page 5.

PRICE: 99.830% AND ACCRUED INTEREST, IF ANY, FROM SEPTEMBER 19, 2013

The Bonds have not been registered under the Securities Act of 1933, as amended (the "Securities Act") or the securities laws of any other jurisdiction. Unless they are registered, the Bonds may be offered only in transactions that are exempt from registration under the Securities Act or the securities laws of any other jurisdiction. Accordingly, the Bonds are being offered and sold only to qualified institutional buyers in compliance with Rule 144A under the Securities Act and outside the United States to persons other than U.S. persons in reliance on Regulation S under the Securities Act. You are hereby notified that sellers of the Bonds may be relying on the exemption from the provisions of Section 5 of the Securities Act provided by Rule 144A. See "Transfer Restrictions."

The Bonds will be ready for delivery in book-entry form through the facilities of The Depository Trust Company ("DTC") for the accounts of its participants, including Euroclear Bank S.A./N.A., as operator of the Euroclear System, and Clearstream Banking, société anonyme, on or about September 19, 2013.

Joint Book-Running Managers

BofA Merrill Lynch

Fifth Third Securities, Inc.

PNC Capital Markets LLC

Morgan Stanley

US Bancorp

Co-Managers

BMO Capital Markets

Regions Securities LLC

Huntington Investment Company

September 12, 2013

TABLE OF CONTENTS

| | |
|--|-----|
| Forward-Looking Statement | iii |
| Where You Can Find More Information | iv |
| Registration Rights; SEC Review | v |
| Summary | 1 |
| The Proposed Offering | 3 |
| Risk Factors | 5 |
| Selected Financial Information | 7 |
| Use of Proceeds | 8 |
| Capitalization | 9 |
| Description of the Bonds | 10 |
| Exchange Offer; Registration Rights | 18 |
| United States Federal Income Tax Consequences | 19 |
| Plan of Distribution | 21 |
| Transfer Restrictions | 24 |
| Legal Matters | 26 |
| Independent Registered Public Accounting Firms | 26 |

This offering memorandum does not constitute an offer to sell, or a solicitation of an offer to buy, any Bonds offered by this offering memorandum to or by any person in any jurisdiction in which it is unlawful for such person to make that offer or solicitation. Neither the delivery of this offering memorandum nor any sale made under this offering memorandum shall under any circumstances imply that there has been no change in our affairs, or that the information set forth in this offering memorandum, including the information incorporated by reference in this offering memorandum, is correct as of any date after the date of this offering memorandum. You should rely only on information contained in this offering memorandum. We have not authorized anyone to provide you with information that is different from that contained in this offering memorandum.

This offering memorandum is highly confidential and has been prepared by us solely for use in connection with this offering. The initial purchasers and we reserve the right to reject any offer to purchase, in whole or in part, for any reason, and the right to sell less than all of the Bonds offered by this offering memorandum. This offering memorandum is personal to the offeree to whom it is delivered by the initial purchasers, and it does not constitute an offer to any other person or to the public in general to subscribe for or otherwise acquire the Bonds or a solicitation of any offer to purchase the Bonds from any other person or the public in general. Distribution of this offering memorandum to any person other than the offeree and those persons, if any, retained to advise that offeree with respect to the offering of the Bonds is unauthorized, and any disclosure of any of its contents, without our prior written consent, is prohibited. Each offeree, by accepting delivery of this offering memorandum, agrees to these restrictions and not to make any copy of this offering memorandum in any medium. Each offeree also agrees that if the offeree does not purchase the Bonds, or the offering is terminated for any reason, the offeree will return this offering memorandum to Merrill Lynch, Pierce, Fenner & Smith Incorporated, Attention: High Grade Capital Markets, One Bryant Park, Floor 3, New York, New York 10036.

Each person receiving this offering memorandum acknowledges that:

- such person was afforded an opportunity to request from us and to review, and has received, all additional information considered by it to be necessary to verify the accuracy of, or to supplement, the information contained or incorporated by reference in this offering memorandum;
- such person did not rely on the initial purchasers or any person affiliated with the initial purchasers in connection with any investigation of the accuracy of such information or its investment decision; and
- no person has been authorized to give any information or to make any representation concerning us or the Bonds (other than as contained or incorporated by reference in this offering memorandum and information given by our duly authorized officers in connection with that investor's examination of us and the terms of this offering) and, if given or made, any such other information or representation should not be relied upon as having been authorized by us or the initial purchasers.

In making an investment decision, investors must rely on their own examination of us and the terms of this offering, including the merits and risks involved. The Bonds have not been recommended by any federal or state securities commission or regulatory authority. Furthermore, the foregoing authorities have not confirmed the accuracy or determined the adequacy of this document. Any representation to the contrary is a criminal offense.

The Bonds are subject to restrictions on transfer and resale and may not be transferred or sold except as permitted under the Securities Act and applicable state securities laws, or pursuant to registration, exemption therefrom or in a transaction not subject thereto. Investors should be aware that they may be required to bear the financial risks of this investment for an indefinite period of time. See "Transfer Restrictions."

No representation or warranty, express or implied, is made by the initial purchasers as to the accuracy or completeness of the information set forth or incorporated by reference in this offering memorandum, and nothing contained or incorporated by reference in this offering memorandum is, or may be relied upon as, a promise or representation, whether as to the past or the future. The initial purchasers assume no responsibility for the accuracy or completeness of the information contained or incorporated by reference in this offering memorandum.

Neither we or any of our representatives nor the initial purchasers or any of their respective representatives is making any representation to any offeree or purchaser of the Bonds offered hereby regarding the legality of an investment by such offeree or purchaser under appropriate legal, tax, business, financial and related aspects of a purchase of the Bonds.

Unless we have indicated otherwise, or the context otherwise requires, for purposes of this offering memorandum (1) references to the "Company," "DP&L," "we," "us," and "our," or similar terms, are to The Dayton Power and Light Company, an Ohio corporation, and (2) references to "DPL" are to DPL Inc., an Ohio corporation, and our parent company.

NOTICE TO NEW HAMPSHIRE RESIDENTS

NEITHER THE FACT THAT A REGISTRATION STATEMENT OR AN APPLICATION FOR A LICENSE HAS BEEN FILED UNDER CHAPTER 421-B OF THE NEW HAMPSHIRE REVISED STATUTES WITH THE STATE OF NEW HAMPSHIRE ("RSA 421-B") NOR THE FACT THAT A SECURITY IS EFFECTIVELY REGISTERED OR A PERSON IS LICENSED IN THE STATE OF NEW HAMPSHIRE CONSTITUTES A FINDING BY THE SECRETARY OF STATE OF NEW HAMPSHIRE THAT ANY DOCUMENT FILED UNDER RSA 421-B IS TRUE, COMPLETE AND NOT MISLEADING. NEITHER ANY SUCH FACT NOR THE FACT THAT AN EXEMPTION OR EXCEPTION IS AVAILABLE FOR A SECURITY OR A TRANSACTION MEANS THAT THE SECRETARY OF STATE OF NEW HAMPSHIRE HAS PASSED IN ANY WAY UPON THE MERITS OR QUALIFICATIONS OF, OR RECOMMENDED OR GIVEN APPROVAL TO, ANY PERSON, SECURITY OR TRANSACTION. IT IS UNLAWFUL TO MAKE, OR CAUSE TO BE MADE, TO ANY PROSPECTIVE PURCHASER, CUSTOMER OR CLIENT ANY REPRESENTATION INCONSISTENT WITH THE PROVISIONS OF THIS PARAGRAPH.

FORWARD-LOOKING STATEMENTS

This offering memorandum and the documents incorporated by reference contain forward-looking statements. Matters discussed in this offering memorandum and the documents incorporated by reference that relate to events or developments that are expected to occur in the future, including management's expectations, strategic objectives, business prospects, anticipated economic performance and financial condition and other similar matters constitute forward-looking statements. Forward-looking statements are based on management's beliefs, assumptions and expectations of future economic performance, taking into account the information currently available to management. These statements are not statements of historical fact and are typically identified by terms and phrases such as "anticipate," "believe," "intend," "estimate," "expect," "continue," "should," "could," "may," "plan," "project," "predict," "will" and similar expressions. Such forward-looking statements are subject to risks and uncertainties and investors are cautioned that outcomes and results may vary materially from those projected due to various factors beyond our control, including but not limited to:

- abnormal or severe weather and catastrophic weather-related damage;
- unusual maintenance or repair requirements;
- changes in fuel costs and purchased power, coal, environmental emissions, natural gas and other commodity prices;
- volatility and changes in markets for electricity and other energy-related commodities;
- generating unit availability and capacity;
- transmission and distribution system reliability and capacity;
- impacts of renewable energy generation, natural gas prices and other factors on whole sale prices;
- changes in our credit ratings or the credit ratings of The AES Corporation ("AES");
- increased competition and deregulation in the electric utility industry;
- increased competition in the retail generation market;
- changes in interest rates;
- state, federal and foreign legislative and regulatory initiatives that affect cost and investment recovery, emission levels, rate structures or tax laws;
- changes in environmental laws and regulations to which we are subject;
- the development and operation of regional transmission organizations, including PJM Interconnection, LLC, to which we have given control of our transmission functions;
- changes in our purchasing processes, pricing, delays, contractor and supplier performance and availability;
- significant delays associated with large construction projects;
- growth in our service territory and changes in demand and demographic patterns;
- changes in accounting rules and the effect of accounting pronouncements issued periodically by accounting standard-setting bodies;
- financial market conditions;
- the outcomes of litigation and regulatory investigations, proceedings or inquiries;
- general economic conditions;
- costs related to the merger through which DPL and we became a wholly-owned subsidiary of AES and the effects of any disruption from the merger that may make it more difficult to maintain relationships with employees, customers, other business partners or government entities; and
- the risks and other factors discussed in this offering memorandum and our filings with the Securities and Exchange Commission ("SEC").

We disclaim any obligation or undertaking to provide any updates or revisions to any forward-looking statement to reflect any change in our expectations or any change in events, conditions or circumstances on which the forward-looking statement is based. If we do update one or more forward-looking statements, no inference should be made that we will make additional updates with respect to those or other forward-looking statements.

WHERE YOU CAN FIND MORE INFORMATION

We file annual and quarterly reports and other information with the SEC. Our filings are available to the public on the Internet on the SEC's web site located at www.sec.gov. You may read and copy any documents we file at the SEC public reference room, 450 Fifth Street, N.W., Washington, D.C. 20549. Call the SEC at 1-800-732-0330 for more information about the public reference room and how to request documents. In addition, for so long as the Bonds remain outstanding, we have agreed to make available to any prospective purchaser of the Bonds the information required by Rule 144A(d)(4) under the Securities Act.

We are "incorporating by reference" the information filed by us with the SEC, which means we can refer you to important information without restating it in this offering memorandum. The information incorporated by reference is an important part of this offering memorandum, and information we file later with the SEC will automatically update and supersede this information. We incorporate by reference into this offering memorandum the following documents that we have filed with the SEC to the limited extent that they reflect information specific to us (we do not incorporate the following documents to the extent that they reflect information specific to our parent company, DPL):

- Annual Report on Form 10-K for the fiscal year ended December 31, 2012, filed with the SEC on February 27, 2013;
- Quarterly Report on Form 10-Q for the fiscal quarter ended March 31, 2013, filed with the SEC on May 9, 2013;
- Quarterly Report on Form 10-Q for the fiscal quarter ended June 30, 2013, filed with the SEC on August 8, 2013; and
- Current Report on Form 8-K, filed with the SEC on May 16, 2013.

In addition, all documents filed by us pursuant to Section 13, 14 or 15(d) of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), subsequent to the date of this offering memorandum and prior to completion of this offering, shall be deemed to be incorporated by reference into this offering memorandum and to be a part of this offering memorandum from the date of filing of such documents.

You may obtain copies of these documents from us, without charge, by calling or writing to us at:

The Dayton Power and Light Company
Attention: Financial Activities
1065 Woodman Drive
Dayton, Ohio 45432
(937) 224-6000

REGISTRATION RIGHTS; SEC REVIEW

We have agreed to file a registration statement with the SEC with respect to an exchange offer to register exchange bonds that have substantially identical terms as the Bonds. See "Exchange Offer; Registration Rights." In the course of the review by the SEC of the registration statement, we may be required or we may elect to make changes to the information contained in this offering memorandum, including the description of our business, financial statements and other financial or other information. We believe that the information included in this offering memorandum has been prepared in a manner that complies, in all material respects, with all requirements of law and practice. However, comments by the SEC on the registration statement may require modification, deletion or reformulation of the information presented in this offering memorandum. Any such modification or reformulation may be significant.

SUMMARY

The following summary is qualified in its entirety by the more detailed information appearing elsewhere in or incorporated by reference into this offering memorandum. The information with respect to us contained in this offering memorandum is only a summary and is not complete. You should read this entire offering memorandum and the documents incorporated by reference in this offering memorandum in their entirety before making an investment decision. You should read the sections entitled "Risk Factors" in this offering memorandum and the documents incorporated by reference herein for more information about important factors that you should consider before buying any Bonds.

The Dayton Power and Light Company

The Dayton Power and Light Company ("DPL") is a public utility incorporated in 1911 under the laws of Ohio. We are engaged in the generation, transmission, distribution and sale of electricity to residential, commercial, industrial and governmental customers in a 6,000 square mile area of West Central Ohio. Electricity sold to standard service offer customers is primarily generated at eight coal-fired power plants. We distribute electricity to more than 513,000 retail customers in our 24 county service area. Principal industries located within our service area include food processing, paper, plastic manufacturing and defense. Our retail generation sales reflect the general economic conditions and seasonal weather patterns of the area as well as retail market conditions. We sell any excess energy and capacity into the wholesale market. We also sell electricity to DPL Energy Resources, Inc., an affiliate, to satisfy the electric requirements of its retail customers.

Our electric transmission and distribution businesses are subject to rate regulation by federal and state regulators, while our generation business is deemed competitive under Ohio law. Accordingly, we apply the accounting standards for regulated operations to our electric transmission and distribution businesses and record regulatory assets when incurred costs are expected to be recovered in future customer rates and regulatory liabilities when current recoveries in customer rates relate to expected future costs.

As of December 31, 2012, we employed approximately 1,400 people. All of our outstanding shares of common stock are held by DPL Inc. ("DPL"), which became our corporate parent, effective April 21, 1986. Our ultimate parent is The AES Corporation ("AES"). Our principal executive and business office is located at 1065 Woodman Drive, Dayton, Ohio 45432 — telephone (937) 224-6000.

Recent Developments

Ohio law requires that all Ohio distribution utilities, such as DPL, file either an electric security plan ("ESP") or market rate option to establish rates for standard service offer ("SSO"), which represents the regulated rates authorized by the Public Utilities Commission of Ohio ("PUCO") and charged to retail customers within the applicable utility's service territory. An ESP, if filed by a utility, may allow for cost-based adjustments to the SSO for costs associated with environmental compliances; fuel and purchased power; construction of new or investment in specified generating facilities; and the provision of standby and default service, operating, maintenance, or other costs including taxes.

On October 5, 2012, we filed an ESP with PUCO to establish SSO rates that were to be in effect starting January 2013. Among other things, the ESP requested approval of a non-bypassable charge of \$137.5 million per year for five years from all customers for the purpose of stabilizing and providing certainty regarding retail electric service by maintaining our financial integrity (a "Service Stability Rider"). On September 6, 2013, the PUCO issued an order on our ESP. The ESP order is subject to reconsideration by the PUCO, upon application by any party to its proceeding, and appellate review by the Ohio Supreme Court. The major elements of the ESP order are listed below, including (i) a requirement to procure an increasing percentage of electricity at market rates, set by a competitive bidding process, blended with electricity at rates established in the ESP order and (ii) a timeline for separating our generation business from our distribution and transmission business in response to Ohio law:

| | |
|--|--|
| ESP Term | January 1, 2014 through May 31, 2017. |
| Service Stability Rider | \$110 million per year (2014-2016). |
| Service Stability Rider Extension | Opportunity to receive \$45.8 million for the period January 1, 2017 through May 31, 2017 if certain conditions are met, including that we must: |

| | |
|-----------------------------------|---|
| | <ul style="list-style-type: none">• demonstrate the amount is necessary for our financial integrity;• file a distribution rate case by July 1, 2014;• file a plan to modernize our electric distribution infrastructure by July 1, 2014;• file an application to divest our generation assets by December 31, 2013; and• establish a plan to modernize our billing system by December 31, 2014. |
| Competitive Bidding Process | Blending percentages: <ul style="list-style-type: none">• January 1, 2014 through December 31, 2014—10%;• January 1, 2015 through December 31, 2015—40%;• January 1, 2016 through May 31, 2017—70%; and• June 1, 2017—100%. |
| Corporate Separation | We are required to file an application to amend our Corporate Separation Plan by December 31, 2013 and are required to complete legal separation of our generation business on or before May 31, 2017. |

The Proposed Offering

The following summary information with respect to this offering is qualified in its entirety by the information contained elsewhere in or incorporated by reference into this offering memorandum.

| | |
|-------------------------------------|---|
| Issuer | The Dayton Power and Light Company. |
| Bonds Offered | \$445,000,000 aggregate principal amount of First Mortgage Bonds, 1.875% Series Due 2016. |
| Maturity | The Bonds will mature on September 15, 2016, unless redeemed prior to that date. |
| Interest Rate | The Bonds will bear interest at 1.875% per annum. |
| Interest Payment Dates | March 15 and September 15 of each year, commencing on March 15, 2014. |
| Optional Redemption | We may redeem the Bonds, in whole or in part, at our option at any time or from time to time prior to maturity, at a redemption price equal to the Make-Whole Amount (as defined below) plus accrued and unpaid interest to the redemption date. The Make-Whole Amount equals the greater of (i) 100% of the principal amount of the Bonds being redeemed or (ii) as determined by a Quotation Agent (as defined below) as of the redemption date, the sum of the present value of the scheduled payments of principal and interest on the Bonds from the redemption date to the stated maturity date of the Bonds (excluding the portion of any such interest accrued to such redemption date), discounted to the redemption date on a semi-annual basis (assuming a 360-day year consisting of twelve 30-day months) at a discount rate equal to the Treasury Rate (as defined below) plus 20 basis points. See "Description of the Bonds—Optional Redemption." |
| Ranking | The Bonds will be senior secured obligations of the Issuer, ranking equally in right of payment with our other existing or future First Mortgage Bonds issued under the First and Refunding Mortgage, dated as of October 1, 1935, between us and the Bank of New York Mellon, as trustee, as amended (the "Mortgage"). See "Description of the Bonds—Priority and Security." |
| Security | The Bonds will be secured by the assets of the Issuer that are currently mortgaged pursuant to the existing Mortgage. See "Description of the Bonds—Priority and Security." |
| Use of Proceeds | The net proceeds from the sale of the Bonds are estimated to be approximately \$438.5 million after deducting the discounts and commissions payable to the initial purchasers and other expenses payable by us. We intend to use the net proceeds from this offering and cash on hand to repay at maturity \$470.0 million aggregate principal amount of our First Mortgage Bonds, 5.125% Series Due 2013. See "Use of Proceeds." |
| Transfer Restrictions | The Bonds have not been registered under the Securities Act or under the securities laws of any other jurisdiction. The Bonds are subject to certain restrictions on transfer and may only be offered or sold in transactions exempt from or not subject to the registration requirements of the Securities Act. See "Transfer Restrictions." |

Exchange Offer; Registration

Rights

Under a registration rights agreement to be executed in connection with this offering, we will agree to file by the date that is 210 days after the date of issuance of the Bonds an exchange offer registration statement registering exchange bonds with the SEC that have substantially identical terms as the Bonds and to use reasonable best efforts to consummate an offer to exchange the exchange bonds for the Bonds on or prior to the date that is 300 days after the date of issuance of the Bonds. We also will agree to file and to use reasonable best efforts to cause to become effective a shelf registration statement relating to the resale of the Bonds under certain circumstances.

We will pay additional interest on the Bonds if the exchange offer is not completed by the applicable date set forth above or if the shelf registration statement is not declared effective by the 90th day after the obligation to file such shelf registration statement arises, in each case, if required, until the completion of the exchange offer, the shelf registration statement is declared effective or the bonds are freely tradable. See "Exchange Offer; Registration Rights."

Trustee and Paying Agent

The Bank of New York Mellon.

RISK FACTORS

In considering whether to purchase the Bonds offered hereby, you should carefully consider the information we have included or incorporated by reference into this offering memorandum. Please see the risk factors discussed in our Annual Report on Form 10-K for the year ended December 31, 2012 and our Quarterly Reports on Form 10-Q for the periods ended March 31, 2013 and June 30, 2013, which are incorporated by reference herein. The risks described in this offering memorandum and in the documents incorporated by reference herein are those that we consider to be the most significant to your decision whether to invest in the Bonds. Additional risks and uncertainties not currently known to us or that we currently deem to be immaterial may also materially and adversely affect our business or results of operations in the future. Any of these risks could materially adversely affect our business, financial condition or results of operations.

Risks Related to the Bonds

We have significant debt, and may not maintain our current credit ratings.

We have a significant amount of debt. Our credit ratings may in the future be lower than our current or historical credit ratings. Differences in credit ratings would affect the interest rates charged on financings, as well as the amounts of indebtedness, types of financing structures and debt markets that may be available to us. In particular, following the order by the Public Utility Commission of Ohio (the "PUCO") on September 6, 2013 with respect to our Electric Security Plan ("ESP"), the rating assigned to us by Moody's was downgraded to Baa3 from Baa2 and the rating assigned to us by Fitch was downgraded to BB+ from 'BBB-. The rating assigned to us by Standard & Poor's remained stable. A downgrade to our existing credit ratings could have a material adverse effect on our operating results and our ability to obtain additional financing, which could adversely affect the market value of the Bonds and could impair our ability to pay interest or principal on the Bonds.

Ratings of the Bonds may change after issuance and affect the market price and marketability of the Bonds.

Bond ratings are limited in scope and do not address all material risks relating to an investment in the Bonds, but rather reflect only the view of each rating agency at the time the rating is issued. An explanation of the significance of a rating may be obtained from the rating agency. There is no assurance that any particular credit ratings will be issued or remain in effect for any given period of time or that such ratings will not be downgraded, suspended or withdrawn entirely by the rating agencies, if, in each rating agency's judgment, circumstances so warrant. Holders of Bonds will have no recourse against us in the event of a change in or suspension or withdrawal of such ratings. Any downgrade, suspension or withdrawal of such ratings may have an adverse effect on the market price or marketability of the Bonds.

The Bonds are not listed on any securities exchange and a liquid market for the Bonds may not develop or be maintained.

We have not listed and we do not intend to list the Bonds on any national securities exchange or to seek their quotation on any automated dealer quotation system. We cannot assure holders of the Bonds that any liquid market for the Bonds will develop or be maintained. The initial purchasers have advised us that they currently intend to make a market in the Bonds following this offering. However, the initial purchasers have no obligation to make a market in the Bonds and they may stop at any time. Further, there can be no assurance as to the liquidity of any market that may develop for the Bonds, holders' ability to sell their Bonds or the price at which holders will be able to sell their Bonds. Future trading prices of the Bonds will depend on many factors, including prevailing interest rates, our financial condition and results of operations, the then-current ratings assigned to the Bonds and the market for similar securities. Any trading market that develops would be affected by many factors independent of and in addition to the foregoing, including the time remaining to the maturity of the Bonds, the outstanding amount of the Bonds, the daily trading volume of the Bonds and the level, direction and volatility of market interest rates generally.

We may choose to redeem the Bonds prior to maturity.

We may redeem the Bonds at any time in whole, or from time to time in part, at a redemption price equal to the Make-Whole-Amount plus accrued and unpaid interest to the redemption date. If prevailing interest rates are lower at the time of redemption, holders of the Bonds may not be able to reinvest the redemption proceeds in a comparable security at an interest rate as high as the interest rate on the Bonds being redeemed. Our redemption right may also adversely affect holders' ability to sell their Bonds. See "Description of the Bonds—Optional Redemption."

The collateral securing the Bonds might not be sufficient to satisfy all the obligations secured by the collateral.

Our obligations under the Bonds are secured by the Mortgage. The Mortgage is also for the benefit of all holders of other series of our first mortgage bonds. See "Description of the Bonds—Priority and Security." As of June 30, 2013, after giving effect to the issuance of the Bonds and the use of proceeds therefrom as described under "Use of Proceeds," we would have had approximately \$859.4 million aggregate principal amount of First Mortgage Bonds outstanding. The value of the Mortgage in the event of a liquidation will depend upon market and economic conditions, the availability of buyers, and similar factors. No independent appraisals of any of the mortgaged property have been prepared by us or on our behalf in connection with this offering. Since no appraisals have been performed in connection with this offering, we cannot assure you that the proceeds of any sale of the mortgaged assets following an acceleration of maturity of the Bonds would be sufficient to satisfy amounts due on the Bonds and the other debt secured by the mortgaged assets.

We have no control over the timing or terms of an order by the PUCO ordering us to separate our generation business into a separate legal entity from our distribution and transmission business.

On September 6, 2013, as a part of its ESP order, the PUCO ordered us to file a revised Corporate Separation Plan by December 31, 2013 and to complete the separation of our generation business on or before May 31, 2017. There can be no assurance of the terms on which the PUCO would authorize the separation of our generation business from our distribution and transmission business. Several regulatory approvals are required in connection with the separation and certain other consents or approvals may be required under other agreements to which we are party, including agreements governing our debt.

SELECTED FINANCIAL INFORMATION

The selected financial data appearing below is qualified in its entirety by reference to, and should be read in conjunction with, our financial statements and related notes that have been incorporated by reference into this offering memorandum. The selected income statement data for the years ended December 31, 2012, 2011 and 2010, and the selected balance sheet data as of December 31, 2012 has been derived from our audited financial statements incorporated by reference herein. The selected income statement data for the years ended December 31, 2009 and 2008 has been derived from our audited financial statements not included herein. The selected income statement data for the six months ended June 30, 2012 and 2013 and the selected balance sheet data as of June 30, 2013 has been derived from our unaudited financial statements incorporated by reference herein. The unaudited selected financial data, in the opinion of management, reflects all adjustments, including normal recurring items, which are necessary to present fairly, in all material respects, the results of interim periods. Operating results for the interim periods presented are not necessarily indicative of the results that may be expected for the entire year or for future periods. Additionally, historical audited financial data is not necessarily indicative of future performance.

| | Six Months Ended June 30, | | Years Ended December 31, | | | | |
|--|------------------------------|---------|--------------------------|-----------|-----------|-----------|-----------|
| | 2013 | 2012 | 2012 | 2011 | 2010 | 2009 | 2008 |
| (\$ in Millions) | | | | | | | |
| Income Statement Data: | | | | | | | |
| Total Revenues | \$728.4 | \$746.2 | \$1,531.8 | \$1,677.7 | \$1,738.8 | \$1,500.8 | \$1,520.5 |
| Operating Income | 98.5 | 122.0 | 185.0 | 319.9 | 450.2 | 421.9 | 436.6 |
| Net Income | 60.5 | 69.4 | 91.2 | 193.2 | 277.7 | 258.9 | 285.8 |
| Ratio of Earnings to Fixed Charges ⁽¹⁾ | 4.8x | 5.9x | 4.5x | 8.2x | 11.4x | 10.1x | 9.8x |

(1) The Ratio of Earnings to Fixed Charges represents, on a pre-tax basis, the number of times earnings cover fixed charges. Earnings consists of income before extraordinary items adding back fixed charges and the provision for income taxes. Fixed charges consists of interest on long-term debt, other interest expense and an estimate of the interest portion of all rentals charged to income.

| | As of June 30, 2013 | As of December 31, 2012 |
|--|---------------------|-------------------------|
| (\$ in Millions) | | |
| Balance Sheet Data: | | |
| Long-Term Debt (including current portion) | \$ 903.1 | \$ 903.1 |
| Preferred Stock Without Mandatory Redemption Provisions | 22.9 | 22.9 |
| Common Shareholder's Equity | <u>1,232.1</u> | <u>1,299.1</u> |

USE OF PROCEEDS

The net proceeds from the sale of the Bonds are estimated to be approximately \$438.5 million after deducting the discounts and commissions payable to the initial purchasers and other expenses payable by us. We intend to use the net proceeds from this offering and cash on hand to repay at maturity \$470.0 million aggregate principal amount of our First Mortgage Bonds, 5.125% Series Due 2013.

CAPITALIZATION

The following table sets forth our cash and cash equivalents, capitalization and short-term debt as of June 30, 2013, (i) on an actual basis and (ii) as adjusted to give effect to the consummation of this offering and the application of the proceeds therefrom. This table should be read in conjunction with "Use of Proceeds" in this offering memorandum and our financial statements that are incorporated by reference herein.

| | As of June 30, 2013 | |
|---|---------------------|-------------|
| | Actual | As Adjusted |
| | (In millions) | |
| Cash and cash equivalents ⁽¹⁾ | \$ 25.4 | \$ 25.4 |
| Short-term debt: | | |
| First Mortgage Bonds maturing in October 2013 - 5.125% | \$ 470.0 | \$ — |
| Long-term debt: | | |
| Unsecured revolving credit facility ⁽²⁾ | — | — |
| Pollution control series maturing in January 2028 - 4.7% ⁽³⁾ | 35.3 | 35.3 |
| Pollution control series maturing in January 2034 - 4.8% ⁽³⁾ | 179.1 | 179.1 |
| Pollution control series maturing in September 2036 - 4.8% ⁽³⁾ | 100.0 | 100.0 |
| Pollution control series maturing in November 2040 - variable rate ⁽³⁾ | 100.0 | 100.0 |
| U.S. Government note maturing in February 2061 - 4.2% | 18.3 | 18.3 |
| First Mortgage Bonds maturing in September 2016 offered hereby - 1.875% | — | 445.0 |
| Total long-term debt | 432.7 | 877.7 |
| Total common shareholder's equity | 1,232.1 | 1,232.1 |
| Total capitalization | \$1,664.8 | \$2,109.8 |

(1) As of August 31, 2013, our cash and cash equivalents was in excess of \$50.0 million.

(2) As of the date of this offering memorandum, our unsecured revolving credit facility remains undrawn.

(3) Each pollution control series represents a series of First Mortgage Bonds that are secured by the same collateral securing the Bonds offered hereby.

DESCRIPTION OF THE BONDS

General

The Bonds are to be issued under the First and Refunding Mortgage, dated as of October 1, 1935, between us and The Bank of New York Mellon, as trustee (the "Trustee"), as amended and supplemented by all supplemental indentures prior to the date hereof and as amended and supplemented by a Forty-Seventh Supplemental Indenture relating to the Bonds (collectively referred to as the "Mortgage").

The statements herein concerning the Bonds and the Mortgage are a summary and do not purport to be complete. The statements make use of defined terms and are qualified in their entirety by express reference to the definitions in, and the appropriate sections and articles of, the Mortgage, a copy of which will be made available upon request to the Trustee.

Maturity, Interest and Payment

The Bonds will mature on September 15, 2016, and will bear interest from the date of original issuance thereof at the rate per annum set forth in their title, payable semi-annually on March 15 and September 15 of each year to bondholders of record at the close of business on the February 28 and August 31 immediately preceding the interest payment date, the first interest payment date being March 15, 2014. The amount of interest payable for any period will be computed on the basis of a 360-day year of twelve 30-day months and for any period shorter than a full month, on the basis of the actual number of days elapsed. In the event that any date on which principal or interest is payable on the Bonds is not a business day, the payment of the principal or interest payable on such date will be made on the next succeeding day which is a business day (and without any interest or other payment in respect of any such delay), with the same force and effect as if made on the date the payment was originally payable. The term "business day" means any day, other than a Saturday or Sunday, or which is not a day on which banking institutions or trust companies in The City of New York are generally authorized or required by law, regulation or executive order to remain closed (or which is not a day on which the corporate trust office of the Trustee is closed for business). We have agreed to pay interest on any overdue principal and, if such payment is enforceable under applicable law, on any overdue installment of interest on the Bonds at the rate per annum set forth in its title.

The Bonds will be issued only in denominations of \$1,000 and integral multiples of \$1,000. We will make principal, premium, if any, and interest payments on the Bonds, other than certificated Bonds, to Cede & Co. (as nominee of The Depository Trust Company ("DTC")) so long as Cede & Co. is the registered owner. Disbursement of such payments to DTC's participants is the responsibility of DTC, and disbursement of such payments to the beneficial owners of the Bonds is the responsibility of DTC participants and indirect participants in DTC, all as described below under "—Book-Entry, Delivery and Form."

The Bonds will not have the benefit of any sinking fund.

Optional Redemption

We may redeem the Bonds, in whole or in part, at any time or from time to time prior to maturity, at a redemption price equal to the Make-Whole Amount, as described below, plus accrued and unpaid interest, if any, to the redemption date with respect to the Bonds, or portion thereof, being redeemed.

The "Make-Whole Amount" shall be equal to the greater of (i) 100% of the principal amount of the Bonds being redeemed or (ii) as determined by the Quotation Agent, as described below, as of the redemption date, the sum of the present values of the scheduled payments of principal and interest on such Bonds from the redemption date to the stated maturity date of the Bonds (excluding the portion of any such interest accrued to such redemption date), discounted to the redemption date on a semi-annual basis (assuming a 360-day year consisting of twelve 30-day months) at a discount rate equal to the Treasury Rate, as described below, plus 20 basis points.

"Treasury Rate" means, with respect to any redemption date, the rate per annum equal to the semi-annual equivalent yield to maturity of the Comparable Treasury Issue, calculated using a price for the Comparable Treasury Issue (expressed as a percentage of its principal amount) equal to the Comparable Treasury Price for such redemption date. The Treasury Rate shall be calculated on the third business day preceding the redemption date.

"Comparable Treasury Issue" means, with respect to any redemption date, the United States Treasury security selected by the Quotation Agent as having a maturity comparable to the time period from the redemption date to the

stated maturity date of the Bonds that would be utilized, at the time of selection and in accordance with customary financial practice, in pricing new issues of corporate debt securities of comparable maturity to the time period. If no United States Treasury security has a maturity which is within a period from three months before to three months after the stated maturity date of the Bonds, the two most closely corresponding United States Treasury securities shall be used as the Comparable Treasury Issue, and the Treasury Rate shall be interpolated and extrapolated on a straight-line basis, rounding to the nearest month using such securities.

“Quotation Agent” means one of the Reference Treasury Dealers selected by us and appointed to act in such role.

“Reference Treasury Dealer” means (i) Merrill Lynch, Pierce, Fenner & Smith Incorporated, Morgan Stanley & Co. LLC and their successors; provided, however, that if any of the foregoing shall cease to be a primary United States Government securities dealer in New York City (a “Primary Treasury Dealer”), we shall substitute therefor another Primary Treasury Dealer and (ii) up to three other Primary Treasury Dealers selected by us.

“Comparable Treasury Price” means (i) the average of the five Reference Treasury Dealer Quotations for such redemption date, after excluding the highest and lowest such Reference Treasury Dealer Quotations, or (ii) if the Quotation Agent obtains fewer than five such Reference Treasury Dealer Quotations, the average of all such Reference Treasury Dealer Quotations.

“Reference Treasury Dealer Quotations” means, with respect to each Reference Treasury Dealer and any redemption date, the average, as determined by the Quotation Agent, of the bid and asked prices for the Comparable Treasury Issue (expressed in each case as a percentage of its principal amount) quoted in writing to the Quotation Agent by such Reference Treasury Dealer at 5:00 p.m., New York City time, on the third business day preceding such redemption date.

Notice of any redemption will be provided at least 20 days but no more than 60 days before the redemption date to each holder of Bonds to be redeemed. If, at the time notice of redemption is given, the redemption monies are not held by the Trustee, the redemption may be made subject to receipt of such monies before the date fixed for redemption, and such notice shall be of no effect unless such monies are so received. Upon payment of the redemption price, on and after the redemption date, interest will cease to accrue on the Bonds or portions thereof called for redemption.

Priority and Security

The Bonds will rank equally and ratably with all other First Mortgage Bonds at any time outstanding under the Mortgage. As of June 30, 2013, after giving effect to the issuance of the Bonds and the use of proceeds therefrom as described under “Use of Proceeds,” we would have had approximately \$859.4 million aggregate principal amount of First Mortgage Bonds outstanding.

All outstanding First Mortgage Bonds will be secured, equally and ratably, by the lien of the Mortgage on substantially all properties owned by us (other than property excepted from such lien and such property as may be released from such lien in accordance with the terms of the Mortgage), and improvements, extensions and additions to, and renewals and replacements of, such properties.

The lien under the Mortgage is subject to certain exclusions, including liens for taxes assessed but not then due or payable, vendor’s liens, liens of purchase money mortgages, liens for paving, conservancy or other assessments, any mortgage or other lien on any property hereafter acquired by us which may exist on the date of such acquisition, prior liens and excepted encumbrances. “Excepted encumbrances” include the following:

- any liens, neither assumed by us nor on which we customarily pay interest charges, existing upon real estate or rights in or relating to real estate we acquired for substation, transmission line, distribution line or right of way purposes;
- rights reserved to or vested in any municipality or public authority by the terms of any franchise, grant, license, permit or by any provision of law to purchase or recapture or to designate a purchaser of any of our property;
- rights reserved to or vested in others to take or receive any part of the power developed or generated by any of our property;
- easements or reservation in any of our property created at or before the time we acquired that property for the purpose of roads, pipe lines, transmission lines and other like purposes;

- rights reserved to or vested in any municipality or public authority to use or control or regulate any of our properties; or
- any obligations or duties affecting our property to any municipality or public authority with respect to any franchise, grant, license or permit.

The Mortgage provides that we will maintain the mortgaged property in working order and condition and equipped with suitable equipment and appliances; that we will make regular charges to expense for the establishment of reasonably adequate reserves for depreciation and will make all needed and proper repairs, retirements, renewals and replacements of the mortgaged property; that we will not charge to our property, plant and equipment accounts any expenditures that are properly chargeable to maintenance or repairs or to any other permitted expense account; and that we may promptly retire property that has permanently ceased to be used or useful in our business.

Release of Property

When not in default, we may obtain the release of any of the mortgaged and pledged property, including, without limiting the generality of the foregoing, any one or more of our heating, gas or water properties substantially as an entirety (provided, however, that our electric property shall not in any event be released substantially as an entirety and, further, that prior lien bonds deposited with the Trustee shall not be released except as provided by the Mortgage) upon deposit with the Trustee of cash equivalent to the amount (if any) by which the value of the property to be released exceeds certain credits, including the cost or fair value, whichever is less, to us of any property additions acquired or constructed prior to or concurrently with such release that have not been used as a basis to issue additional First Mortgage Bonds. Money received by the Trustee upon any release may be withdrawn against property additions or against the deposit of bonds or prior lien bonds, or at our request, may be applied to purchase First Mortgage Bonds or to redeem First Mortgage Bonds that are redeemable by their terms at that time.

“Property additions” means property acquired or constructed after September 30, 1945, to be used in the electric, natural gas, steam or water business.

“Funded property” includes property additions used to satisfy requirements of bond issuances and obligations or bond retirements.

Issuance of Additional First Mortgage Bonds

The Mortgage permits us to issue an unlimited amount of First Mortgage Bonds from time to time in one or more series. All First Mortgage Bonds of one series need not be issued at the same time, and a series may be reopened for issuances of additional First Mortgage Bonds of such series. This means that we may from time to time, without the consent of the existing holders of the Bonds, create and issue additional First Mortgage Bonds having the same terms and conditions as the Bonds in all respects, except for issue date, issue price and, if applicable, the initial interest payment on the Bonds. Additional First Mortgage Bonds issued in this manner will be consolidated with, and will form a single series with, the previously outstanding First Mortgage Bonds of such series, including, if applicable, the Bonds.

Additional First Mortgage Bonds, including additional First Mortgage Bonds of an existing series, may be issued:

- (1) upon the basis of property additions which are not then funded property in a principal amount which, together with any prior lien bonds outstanding on such property additions, will not exceed 60% of the cost or fair value to us of such property additions, whichever is less;
- (2) against deposits or retirement of prior lien bonds deducted in determining the amount of First Mortgage Bonds issuable upon the basis of property additions;
- (3) upon payment or retirement of other First Mortgage Bonds issued under the Mortgage or upon deposit with the Trustee of the money necessary for their purchase or payment, in principal amount equivalent to the First Mortgage Bonds paid or retired, or for which money has been so deposited; or
- (4) upon deposit with the Trustee of cash equal to the principal amount of the First Mortgage Bonds to be issued; such cash may be withdrawn in lieu of First Mortgage Bonds, which we may be entitled to have authenticated and delivered to us.

The issuance of additional First Mortgage Bonds is also limited by a net earnings test, under which no First Mortgage Bonds may be issued upon the basis of property additions or under certain other circumstances unless our adjusted

net earnings for 12 consecutive calendar months in the 18 calendar months preceding the application for the issue of such First Mortgage Bonds shall be at least two times annual interest charges on all First Mortgage Bonds outstanding (except any for the payment of which the First Mortgage Bonds applied for are to be issued), on the additional First Mortgage Bonds and on the principal amount of all other indebtedness (except indebtedness for the payment of which the First Mortgage Bonds applied for are to be issued and indebtedness for the purchase, payment or redemption of which moneys in the necessary amount shall have been deposited with or be held by the Trustee or the trustee or other holder of a lien prior to the lien of the Mortgage upon property subject to the lien of the Mortgage with irrevocable direction so to apply the same; provided that, in the case of redemption, the notice required therefor shall have been given or have been provided for to the satisfaction of the Trustee), outstanding in the hands of the public and secured by a lien prior to the lien of the Mortgage upon property subject to the lien of the Mortgage, if said indebtedness has been assumed by us or if we customarily pay the interest upon the principal thereof.

As of December 31, 2012, the amount (the lesser of cost or fair value) of property additions which we could use as a basis for the issuance of additional First Mortgage Bonds was approximately \$2.39 billion. Under the property additions test, we would have been permitted at December 31, 2012 to issue approximately \$1.43 billion of First Mortgage Bonds. In addition, at such date, approximately \$148.7 million of First Mortgage Bonds would have been permitted to be issued as a result of prior bond retirements. The Bonds will be issued upon the basis of property additions.

Modification of Mortgage

Our rights and obligations and those of the holders of the First Mortgage Bonds may be modified upon the written consent of the holders of at least a majority of the First Mortgage Bonds then outstanding, but no such modification shall extend the maturity of or reduce the rate of interest on or otherwise modify the terms of payment of principal of or interest on First Mortgage Bonds or permit the creation of any lien ranking prior to or equal with the lien of the Mortgage on any of the mortgaged property. If any proposed modification shall affect the rights of holders of the First Mortgage Bonds of one or more, but not all, series, then only holders of First Mortgage Bonds of the series to be affected shall be required to consent to or shall have authority to approve such modification. Any waiver of a completed default shall be deemed to affect the First Mortgage Bonds of all series, and, subject to the foregoing, any modification of the provisions of any sinking fund established in respect of a particular series shall be deemed to affect only the First Mortgage Bonds of that series. The determination of the Trustee as to what series of First Mortgage Bonds are affected by any modification shall be conclusive.

Events of Default

Among the events which constitute a "completed default" by us under the Mortgage are the following: (a) default in the payment of the principal of any First Mortgage Bond; (b) default for 90 days in the payment of interest on any First Mortgage Bond; (c) default for 90 days in the payment of amounts required for any sinking fund established in respect of a particular series; (d) certain events in bankruptcy, insolvency or reorganization; and (e) default, for 90 days after notice to us from the Trustee, in the performance of any other covenant, agreement or condition contained in the Mortgage. Upon the occurrence of any such completed default, the Trustee or the holders of not less than 25% in principal amount of the First Mortgage Bonds of all series outstanding under the Mortgage may declare the principal of, and any accrued interest on, all such First Mortgage Bonds immediately due and payable, subject to the right of the holders of a majority in principal amount of all such First Mortgage Bonds to annul such declaration if before any sale of the mortgaged property the default is cured. We are not required to furnish periodically to the Trustee evidence as to the absence of default or as to compliance with the terms of the Mortgage, but such evidence is required in connection with the issuance of any additional First Mortgage Bond under the Mortgage and in certain other circumstances. In addition, we are required by law to furnish annually to the Trustee a certificate as to compliance with all conditions and covenants under the Mortgage.

No bondholder may institute any action, suit or proceeding for any remedy under the Mortgage unless it shall have previously given to the Trustee written notice of a default by us and, in addition, (i) the holders of not less than 25% in principal amounts of the First Mortgage Bonds outstanding under the Mortgage shall have made a written request to the Trustee to exercise its powers under the Mortgage or to institute such action, suit or proceeding in its own name, (ii) such holders shall have offered to the Trustee security and indemnity satisfactory to it against the costs, expenses and liabilities to be incurred thereby and (iii) the Trustee shall have refused to exercise such powers or to institute such action in its own name or shall have failed to do so for an unreasonable time. Bondholders, however, have an absolute and unconditional right, without such notice to the Trustee, to enforce the payment of the principal of and the interest on their First Mortgage Bonds at and after the maturity thereof.

No personal liability of directors, officers, employees, managers and stockholders

No personal liability whatever shall attach to, or be incurred by, any incorporator or any past, present or future subscriber to capital stock, stockholder, officer or director of the Company or of any predecessor or successor corporation, or any of them, because of the incurring of the indebtedness authorized by the Mortgage, or under or by reason of any of the obligations, covenants or agreements contained in the Mortgage or in any indenture supplemental thereto or in any of the First Mortgage Bonds, or implied therefrom. Each holder of First Mortgage Bonds by accepting a First Mortgage Bond waives and releases all such liability. The waiver and release are part of the consideration for issuance of the First Mortgage Bonds. The waiver may not be effective to waive liabilities under the federal securities laws.

Satisfaction and Discharge of the Mortgage

Upon our making due provision for the payment of all First Mortgage Bonds and paying all other sums due under the Mortgage, the Mortgage shall cease to be of further effect and may be satisfied and discharged of record.

Merger, Consolidation and Sale

Subject to the conditions listed in the next paragraph, we may consolidate with or merge into any corporation having corporate authority to carry on any of the businesses of generating, manufacturing, transmitting, distributing or supplying (i) electricity or gas for light, heat, power or other purposes, (ii) steam or hot water for power or heat or other purposes or (iii) water for domestic or public use and consumption. The Mortgage also allows conveyance or transfer of all of the mortgaged and pledged property substantially as an entirety to any corporation that is lawfully entitled to acquire and operate such property.

The consolidation, merger, conveyance or transfer of all of the mortgaged and pledged property substantially as an entirety must satisfy the following conditions: (i) it must be upon such terms as to preserve and in no respect impair the lien or security of the Mortgage, or any rights or powers of the Trustee or the holders of First Mortgage Bonds; and (ii) the person formed by such consolidation, or into which we shall have been merged, or acquiring all the mortgaged and pledged property substantially as an entirety must expressly assume in writing the due and punctual payment of the principal and interest of all First Mortgage Bonds and the due and punctual performance and observance of all covenants and conditions of the Mortgage.

After such consolidation, merger, conveyance or transfer, the lien of the Mortgage will generally not cover the property of the successor corporation, other than the property that it acquires from us with certain exceptions.

Dividend Covenant

The Mortgage does not restrict our ability to pay dividends on our common stock.

Defeasance

Any Bonds, or any portion of the principal amount thereof, will be deemed to have been paid for all purposes of the Mortgage, and the entirety of our indebtedness in respect thereof will be deemed to have been satisfied and discharged, if there has been irrevocably deposited with the Trustee or any paying agent (other than us) for such purpose, in trust:

- money (including funded cash not otherwise applied pursuant to the Mortgage, to the extent permitted by the Mortgage) in an amount which will be sufficient; or
- in the case of a deposit made prior to the date on which principal is due, eligible obligations (as described below), which do not contain provisions permitting the redemption or other prepayment thereof at the option of the issuer thereof, the principal of and the interest on which when due, without any regard to reinvestment thereof, will provide monies which, together with the money, if any, deposited with or held by the trustee or such paying agent pursuant to the first bullet point, will be sufficient; or
- a combination of options in the preceding bullet points,

which in each case, will be sufficient, without reinvestment, in the opinion of a nationally recognized investment bank, appraisal firm or firm of independent public accountants expressed in a written certification delivered to the Trustee, to pay when due the principal of and premium, if any, and interest, if any, due and to become due on such

Bonds or portions thereof. For this purpose, eligible obligations include direct obligations of, or obligations unconditionally guaranteed by, the United States of America, entitled to the benefit of the full faith and credit thereof, and certificates, depository receipts or other instruments, which may be issued by the Trustee that evidence a direct ownership interest in such obligations or in any specific interest or principal payments due in respect thereof.

Notwithstanding the foregoing, no Bond shall be deemed to have been paid as aforesaid unless we shall have delivered to the Trustee either:

- an opinion of counsel in the United States who is reasonably acceptable to the Trustee confirming that (i) we have received from, or there has been published by, the Internal Revenue Service a ruling or (ii) since the date of the Mortgage, there has been a change in the applicable federal income tax law, in either case to the effect that, and based thereon such opinion of counsel shall confirm that, the holders of the outstanding Bonds will not recognize income, gain or loss for federal income tax purposes as a result of such defeasance and will be subject to federal income tax on the same amounts, in the same manner and at the same times as would have been the case if such defeasance had not occurred; or
- an instrument wherein we, notwithstanding the satisfaction and discharge of our indebtedness in respect of Bonds, shall assume the obligation (which shall be absolute and unconditional) to irrevocably deposit with the Trustee such additional sums of money, if any, or additional eligible obligations, if any, or any combination thereof, at such time or times, as shall be necessary, together with the money and/or eligible obligations theretofore so deposited, to pay when due the principal of and premium, if any, and interest due and to become due on such Bonds or portions thereof; provided, however, that such instrument may state that our obligation to make additional deposits as aforesaid shall be subject to the delivery to us by a holder of a Bond of a notice asserting the deficiency accompanied by an opinion of an independent public accountant of nationally recognized standing showing the calculation thereof; and
- an opinion of tax counsel in the United States who is reasonably acceptable to the Trustee to the effect that the holders of the outstanding Bonds will not recognize income, gain or loss for federal income tax purposes as a result of such defeasance and will be subject to federal income tax on the same amounts, in the same manner and at the same times as would have been the case if such defeasance had not occurred.

Regarding the Trustee

The Trustee under the Mortgage is The Bank of New York Mellon. We, DPL, AES and their other subsidiaries also maintain various banking, lending, trust and other relationships with The Bank of New York Mellon and its affiliates.

The Mortgage provides that our obligations to compensate the Trustee and reimburse the Trustee for expenses (including any indemnity obligations) will be secured by a lien generally prior to that of the First Mortgage Bonds on the Mortgage trust estate and the proceeds thereof.

Book-Entry, Delivery and Form

The Bonds will be issued in the form of fully registered securities in global form (the "global securities"). The global securities will be deposited with, or on behalf of, DTC, or the depository, and registered in the name of the depository or its nominee.

Upon issuance of the global securities, the depository or its nominee will credit, on its book entry registration and transfer system, the number of Bonds sold to QIBs pursuant to Rule 144A represented by such global securities and the number of Bonds sold to certain persons in offshore transactions in reliance on Regulation S under the Securities Act represented by such global securities to the account of institutions that have accounts with the depository or its nominee participants (the "DTC participants"), including indirectly to the accounts of institutions that have accounts with the Euroclear Bank S.A./N.A. as operator of the Euroclear System and Clearstream Banking, société anonyme, or their respective nominee participants (the "Euroclear and Clearstream participants" and, collectively with the DTC participants, the "participants"). The accounts to be credited shall be designated by the initial purchasers. Prior to the 40th day after the closing date, any resale or transfer of beneficial interests in the Regulation S global securities will not be permitted during that period unless the resale or transfer is made pursuant to Rule 144A or Regulation S. Ownership of beneficial interests in the global securities will be limited to participants or persons that may hold interests through participants. Ownership of beneficial interests in such global securities will be shown on, and the transfer of that ownership will be effected only through, records maintained by the depository or its nominee (with respect to the participants' interests) for such global securities, or by participants or persons that hold interests through

participants (with respect to beneficial interests of persons other than participants). The laws of some jurisdictions may require that certain purchasers of securities take physical delivery of such securities in definitive form. Such limits and laws may impair the ability to transfer or pledge beneficial interests in the global securities. Investors may hold their interests in a Regulation S global security directly through Clearstream or Euroclear, if they are participants in those systems, or indirectly through organizations that are participants in those systems. Clearstream and Euroclear will hold interests in the Regulation S global securities on behalf of their participants through the depositary.

So long as the depositary, or its nominee, is the registered holder of any global securities, the depositary or such nominee, as the case may be, will be considered the sole legal owner of such securities for all purposes under the Mortgage and the Bonds. Except as set forth below, owners of beneficial interests in global securities will not be entitled to have such global securities registered in their names, will not receive or be entitled to receive physical delivery in exchange therefor and will not be considered to be the owners or holders of such global securities for any purpose under the Bonds or the Mortgage. We understand that under existing industry practice, in the event an owner of a beneficial interest in a global security desires to take any action that the depositary, as the holder of such global security, is entitled to take, the depositary would authorize the participants to take such action, and that the participants would authorize beneficial owners owning through such participants to take such action or would otherwise act upon the instructions of beneficial owners owning through them.

Any payment of principal, premium, if any, or interest due on the Bonds on any interest payment date, redemption date, or at maturity will be made available by us to the Trustee by such date. As soon as possible thereafter, the Trustee will make such payments to the depositary or its nominee, as the case may be, as the registered owner of the global securities representing such Bonds in accordance with existing arrangements between the Trustee and the depositary.

We expect that the depositary or its nominee, upon receipt of any payment of principal, premium or interest in respect of the global securities, will credit immediately the accounts of the related participants with payments in amounts proportionate to their respective beneficial interests in the principal amount of such global security as shown on the records of the depositary. We also expect that payments by participants to owners of beneficial interests in the global securities held through such participants will be governed by standing instructions and customary practices, as is now the case with securities held for the accounts of customers in bearer form or registered in "street name" and will be the responsibility of such participants.

Transfers between participants in the depositary will be effected in the ordinary way in accordance with the depositary's rules and will be settled in same-day funds. Transfers between Euroclear and Clearstream participants will be effected in the ordinary way in accordance with their respective rules and operating procedures.

None of us, the Trustee, or any paying agent for the global securities will have any responsibility or liability for any aspect of the records relating to or payments made on account of beneficial ownership interests in any of the global securities or for maintaining, supervising or reviewing any records relating to such beneficial ownership interests or for other aspects of the relationship between the depositary and its participants or the relationship between such participants and the owners of beneficial interests in the global securities owning through such participants.

Unless and until exchanged in whole or in part for securities in definitive form in accordance with the terms of the Bonds, the global securities may not be transferred except as a whole by the depositary to a nominee of the depositary or by a nominee of the depositary to the depositary or another nominee of the depositary or by the depositary of any such nominee to a successor of the depositary or a nominee of each successor.

Settlement for the Bonds will be made by the initial purchasers in immediately available funds. So long as the depositary continues to make its settlement system available to us, all payments of principal of, premium, if any, and interest on the global securities will be made by us in immediately available funds.

Although the depositary has agreed to the foregoing procedures in order to facilitate transfers of interests in the global securities among participants of the depositary, it is under no obligation to perform or continue to perform such procedures, and such procedures may be discontinued at any time. Neither the Trustee nor we will have any responsibility for the performance by the depositary or its participants or indirect participants of their respective obligations under the rules and procedures governing their operations. We and the Trustee may conclusively rely on, and shall be protected in relying on, instructions from the depositary for all purposes.

The global securities shall be exchangeable for corresponding certificated Bonds registered in the name of persons other than the depositary or its nominee only if (a) the depositary (i) notifies us that it is unwilling or unable to

continue as depositary for any of the global securities or (ii) at any time ceases to be a clearing agency registered under the Exchange Act, (b) there shall have occurred and be continuing an event of default under the Mortgage with respect to the related series of Bonds or (c) we execute and deliver to the Trustee, an order that the global securities shall be so exchangeable. Any certificated Bonds will be issued only in fully registered form and shall be issued without coupons in minimum denominations of \$1,000 and in integral multiples of \$1,000 in excess thereof. Any certificated Bonds so issued will be registered in such names as the depositary shall request.

Principal, premium, if any, and interest on all certificated Bonds in registered form will be payable at the office or agency of the Trustee in The City of New York, except that, at our option, payment of any interest (except interest due at maturity) may be made by check mailed to the address of the person entitled thereto as such address shall appear in the security register or by wire transfer to an account maintained by the person entitled thereto as specified in the security register.

The depositary has advised us as follows: The depositary is a limited-purpose trust company organized under the laws of the State of New York, a member of the Federal Reserve System, a "clearing corporation" within the meaning of the New York Uniform Commercial Code and "a clearing agency" registered under the Exchange Act. The depositary was created to hold securities of institutions that have accounts with the depositary and to facilitate the clearance and settlement of securities transactions among its participants in such securities through electronic book-entry changes in accounts of participants, thereby eliminating the need for physical movement of securities certificates. The depositary's participants include securities brokers and dealers (which may include the initial purchasers), banks, trust companies, clearing corporations and certain other organizations some of whom (or their representatives) own DTC. Access to the depositary's book-entry system is also available to others such as banks, brokers, dealers and trust companies that clear through or maintain a custodial relationship with a participant, whether directly or indirectly.

EXCHANGE OFFER; REGISTRATION RIGHTS

We have agreed with the initial purchasers, for the benefit of the holders of the Bonds, to use our reasonable best efforts, at our cost, to file, by the date that is 210 days after the date of issuance of the Bonds, and cause to become effective a registration statement with respect to a registered offer to exchange the Bonds for an issue of Bonds of ours ("exchange notes") with terms substantially identical to the Bonds (except that the exchange notes will not be subject to transfer restrictions) and to use reasonable best efforts to consummate the offer to exchange the exchange bonds for the Bonds on or prior to the date that is 300 days after the date of issuance of the Bonds. Upon the exchange offer registration statement being declared effective, we will offer the exchange notes in return for surrender of the Bonds. The offer will remain open for not less than 20 business days after the date notice of the exchange offer is sent to holders. For each Bond surrendered to us under the exchange offer, the holder will receive an exchange note of equal principal amount. Interest on each exchange note will accrue from the last interest payment date on which interest was paid on the Bonds so surrendered (or if the exchange note is authenticated between a record date and interest payment date, from such interest payment date) or, if no interest has been paid on the Bonds, from the issue date of the Bonds.

A holder of Bonds that wishes to exchange the Bonds for exchange notes in the exchange offer will be required to represent, among other things, that (i) any exchange notes received by such holder will be acquired in the ordinary course of its business, (ii) it has no arrangement or understanding with any person to participate in the distribution of the Bonds within the meaning of the Securities Act, (iii) if the holder is not a broker-dealer or is a broker-dealer but will not receive exchange notes for its own account in exchange for the Bonds, neither the holder nor any such other person is engaged in or intends to participate in a distribution of the exchange securities and (iv) it is not an affiliate (as defined in Rule 501(b) under the Securities Act) of ours.

If applicable interpretations of the staff of the SEC do not permit us to effect the exchange offer, or under certain other circumstances, we will, at our cost, use our reasonable best efforts to cause to become effective a shelf registration statement with respect to resales of the Bonds and to keep the registration statement effective for a period of one year after the issue date of the Bonds, or, if earlier, the date when all Bonds covered by the shelf registration statement have been sold pursuant to the shelf registration statement. We will, in the event of a shelf registration, provide copies of the prospectus to each holder, notify each holder when the shelf registration statement for the Bonds has become effective and take certain other actions as are required to permit resales of the Bonds. A holder that sells its Bonds pursuant to the shelf registration statement generally will be required to be named as a selling security holder in the related prospectus and to deliver a prospectus to purchasers, will be subject to certain of the civil liability provisions under the Securities Act in connection with those sales and will be bound by the provisions of the registration rights agreement that are applicable to a selling holder, including certain indemnification obligations.

If (a) we do not consummate the exchange offer on or prior to the date that is 300 days following the issuance of the Bonds (the "exchange offering closing deadline") or (b) we have not caused to become effective a shelf registration statement by the 90th day after the obligation to file such shelf registration statement arises (the "shelf effectiveness deadline") (which in no event, however, shall be earlier than the exchange offer closing deadline (each such event referred to in clause (a) and (b) a "Registration Default")), the interest rate for the Bonds will increase by 0.25% per annum during the first 90-day period immediately following the occurrence of any Registration Default, and such increased rate will further increase by 0.25% per annum beginning on the 91st day following the occurrence of such Registration Default, but in no event shall such increases (such amounts "additional interest") exceed in the aggregate 0.50% per annum regardless of the number of Registration Defaults that have occurred and are continuing. Following the cure of all Registration Defaults, the interest rate on the Bonds will be reduced to the original interest rate; provided, however, that, if after any such reduction in interest rate, a different Registration Default occurs, the interest rate on the Bonds shall again be increased pursuant to the foregoing provisions.

If we effect the exchange offer, we will be entitled to close the exchange offer 20 business days after the commencement thereof (but in no event more than 60 days after commencement) if we have accepted all Bonds validly surrendered in accordance with the terms of the exchange offer. Bonds not tendered in the exchange offer will bear interest at the rate set forth on the cover page of this offering memorandum and be subject to all of the terms and conditions specified in the indenture and to the transfer restrictions described in "Transfer Restrictions."

This is a summary of the material provisions of the registration rights agreement. Because this is a summary, it may not contain all the information that is important to you. You should read the registration rights agreement in its entirety. Copies of the proposed form of registration rights agreement are available as described under "Where You Can Find More Information."

UNITED STATES FEDERAL INCOME TAX CONSEQUENCES

The following is a general discussion of U.S. federal income tax consequences of the purchase, ownership and disposition of the Bonds by a Non-U.S. Holder (as defined below) that purchases the Bonds pursuant to this offering. This summary is based upon U.S. federal income tax law in effect on the date of this offering memorandum, which may be subject to differing interpretations or change, possibly with retroactive effect. This summary does not discuss all aspects of U.S. federal income taxation that may be important to particular investors in light of their individual investment circumstances, such as investors subject to special tax rules (e.g., financial institutions, certain former citizens and former long-term residents of the United States, "controlled foreign corporations," and "passive foreign investment companies"), persons that will hold the Bonds as a part of a larger transaction, or partnerships (as described below), all of whom may be subject to tax rules that differ significantly from those summarized below. This summary addresses investors who will hold the Bonds as "capital assets" (generally, property held for investment) under the Internal Revenue Code of 1986, as amended (the "Code"), and does not discuss state, local, or non-U.S. tax considerations. **Each prospective investor is urged to consult its tax advisor regarding the U.S. federal, state, local and non-U.S. income and other tax considerations of the purchase, ownership and disposition of the Bonds.**

For the purposes of this summary, a "Non-U.S. Holder" is a beneficial owner of the Bonds that, for U.S. federal income tax purposes, is not (i) an individual who is a citizen or resident of the United States, (ii) a partnership or corporation created in, or organized under the law of, the United States or any state thereof or the District of Columbia, (iii) an estate the income of which is includible in gross income for U.S. federal income tax purposes regardless of its source, or (iv) a trust (A) the administration of which is subject to the primary supervision of a U.S. court and which has one or more United States persons who have the authority to control all of the substantial decisions of the trust or (B) that has otherwise elected to be treated as a United States person under the Code.

If a partnership (including an entity or arrangement treated as a partnership for U.S. federal income tax purposes) holds the Bonds, the tax treatment of a partner in the partnership generally will depend upon the status of the partner and the activities of the partnership. If you are a partnership considering the purchase of the Bonds pursuant to this offering, you are urged to consult your tax advisor.

To ensure compliance with U.S. Treasury Department Circular 230, holders are hereby notified that: (i) any discussion of U.S. federal tax issues in this offering memorandum is not intended or written to be used, and cannot be used by such holders for the purpose of avoiding penalties that may be imposed on such holders under the Code; (ii) this discussion is being used in connection with the promotion or marketing (within the meaning of Circular 230) of the transactions or matters discussed herein; and (iii) holders should seek advice based on their particular circumstances from an independent tax advisor.

Interest income

Payments of interest on the Bonds made to a Non-U.S. Holder will not be subject to U.S. federal income or withholding tax provided that (i) such interest is not effectively connected with the conduct of a trade or business within the United States (or, if certain tax treaties apply, such interest is not attributable to a permanent establishment or fixed base maintained within the United States by the Non-U.S. Holder) and (B) such Non-U.S. Holder (1) does not actually or constructively own 10% or more of the total combined voting power of all classes of our stock entitled to vote and (2) is not a controlled foreign corporation that is related to us (within the meaning of the Code) and (ii) certain certification requirements are satisfied. Such certification requirements will be met if (i) the Non-U.S. Holder provides its name and address, and certifies on an Internal Revenue Service ("IRS") Form W-8BEN (or appropriate substitute form), under penalties of perjury, that it is not a United States person or (ii) a securities clearing organization, bank or certain other financial institutions holding the Bonds on behalf of the Non-U.S. Holder certifies on IRS Form W-8IMY, under penalties of perjury, that the certification referred to in clause (i) has been received by it and furnishes us or our paying agent with a copy thereof. In addition, we or our paying agent must not have actual knowledge or reason to know that the beneficial owner of the Bonds is a United States person or that any of the information, certifications or statements in the IRS Form W-8BEN are incorrect.

If a Non-U.S. Holder cannot satisfy these requirements and interest on the Bonds is not effectively connected with the conduct of a trade or business within the United States, payments of interest generally will be subject to U.S. federal withholding tax at a 30% rate (or a lower applicable treaty rate, provided certain certification requirements are met). If interest on the Bonds is effectively connected with the conduct of a trade or business within the United States by a Non-U.S. Holder (and, if certain tax treaties apply, such interest is attributable to a permanent estab-

lishment or fixed base within the United States), then the Non-U.S. Holder will generally be subject to U.S. federal income tax on the receipt or accrual of such interest on a net income basis in the same manner as if such holder were a United States person, and, in the case of a Non-U.S. Holder that is a foreign corporation, may also be subject to an additional branch profits tax, currently imposed at a rate of 30% (or a lower applicable treaty rate), on its effectively connected earnings and profits, subject to adjustments. Any such interest will not also be subject to U.S. federal withholding tax, however, if the Non-U.S. Holder delivers to us a properly executed IRS Form W-8ECI in order to claim an exemption from U.S. federal withholding tax.

Sale, exchange, redemption or other taxable disposition

A Non-U.S. Holder will generally not be subject to U.S. federal income tax (or any withholding thereof) with respect to gain, if any, recognized on the sale, exchange, redemption or other taxable disposition of the Bonds unless (1) the gain is effectively connected with the conduct of a trade or business within the United States by the Non-U.S. Holder (and, if certain tax treaties apply, is attributable to a permanent establishment or fixed base of the Non-U.S. Holder within the United States), or (2) in the case of a Non-U.S. Holder that is an individual, such holder is present in the United States for 183 or more days in the taxable year in which such sale, exchange, redemption or other taxable disposition occurs and certain other conditions are satisfied.

Gain that is effectively connected with the conduct of a trade or business in the United States will generally be subject to U.S. federal income tax on a net income basis (but not U.S. withholding tax), in the same manner as if the Non-U.S. Holder were a United States person, and, in the case of a Non-U.S. Holder that is a foreign corporation, may also be subject to an additional branch profits tax, currently imposed at a rate of 30% (or a lower applicable treaty rate), on its effectively connected earnings and profits, subject to adjustments. An individual Non-U.S. Holder who is subject to U.S. federal income tax because the Non-U.S. Holder was present in the United States for 183 days or more during the year of sale, exchange, redemption, or other disposition of the Bonds will be subject to a flat 30% tax on the gain derived from such sale or other taxable disposition, which may be offset by certain U.S. source capital losses.

Backup withholding and information reporting

A Non-U.S. Holder will generally be required to comply with certain certification procedures to establish that such holder is not a United States person in order to avoid backup withholding with respect to payments of principal and interest on, or the proceeds from a disposition of, the Bonds. Such requirement will be satisfied if the Non-U.S. Holder delivers the appropriate IRS Form W-8 as described above. In addition, we must report annually to the IRS and to each Non-U.S. Holder the amount of any interest paid to such Non-U.S. Holder regardless of whether any tax was actually withheld. Copies of the information returns reporting such interest payments and the amount withheld may also be made available to the tax authorities in the country in which a Non-U.S. Holder resides under the provisions of an applicable tax treaty.

Backup withholding is not an additional tax. Any amounts withheld under the backup withholding rules will be allowed as a refund or credit against a Non-U.S. Holder's U.S. federal income tax liability, provided the required information is correctly and timely provided to the IRS.

PLAN OF DISTRIBUTION

Merrill Lynch, Pierce, Fenner & Smith Incorporated, Morgan Stanley & Co. LLC, Fifth Third Securities, Inc., PNC Capital Markets LLC and U.S. Bancorp Investments, Inc. are acting as joint book-running managers of the offering. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Morgan Stanley & Co. LLC are acting as representatives of the several initial purchasers. Subject to the terms and conditions stated in a purchase agreement among us and the initial purchasers, each initial purchaser named below has severally agreed to purchase, and we have agreed to sell to that initial purchaser, the principal amount of the Bonds set forth opposite the initial purchaser's name.

| <u>Initial Purchaser</u> | <u>Principal Amount of the Bonds</u> |
|---|--|
| Merrill Lynch, Pierce, Fenner & Smith Incorporated | \$ 94,562,500 |
| Morgan Stanley & Co. LLC | 94,562,500 |
| Fifth Third Securities, Inc. | 66,750,000 |
| PNC Capital Markets LLC | 66,750,000 |
| U.S. Bancorp Investments, Inc. | 66,750,000 |
| BMO Capital Markets GKST Inc. | 22,250,000 |
| The Huntington Investment Company | 22,250,000 |
| Regions Securities LLC | 11,125,000 |
| Total | <u>\$445,000,000</u> |

Subject to the terms and conditions set forth in the purchase agreement, the initial purchasers have agreed, severally and not jointly, to purchase all of the Bonds sold under the purchase agreement if any of these Bonds are purchased. If an initial purchaser defaults, the purchase agreement provides that the purchase commitments of the nondefaulting initial purchasers may be increased or the purchase agreement may be terminated.

We have agreed to indemnify the initial purchasers and their controlling persons against certain liabilities in connection with this offering, including liabilities under the Securities Act, or to contribute to payments the initial purchasers may be required to make in respect of those liabilities.

The initial purchasers are offering the Bonds, subject to prior sale, when, as and if issued to and accepted by them, subject to approval of legal matters by their counsel, including the validity of the Bonds, and other conditions contained in the purchase agreement, such as the receipt by the initial purchasers of officers' certificates and legal opinions. The initial purchasers reserve the right to withdraw, cancel or modify offers to the public and to reject orders in whole or in part.

Bonds are not Being Registered

The initial purchasers propose to offer the Bonds for resale in transactions not requiring registration under the Securities Act or applicable state securities laws, including sales pursuant to Rule 144A. The initial purchasers will not offer or sell the Bonds except:

- to persons they reasonably believe to be qualified institutional buyers; or
- pursuant to offers and sales to non-U.S. persons that occur outside the United States within the meaning of Regulation S.

Bonds sold pursuant to Regulation S may not be offered or resold in the United States or to U.S. persons (as defined in Regulation S), except under an exemption from the registration requirements of the Securities Act or under a registration statement declared effective under the Securities Act.

Each purchaser of the Bonds will be deemed to have made acknowledgments, representations and agreements as described under "Transfer Restrictions."

New Issue of Bonds

The Bonds constitute a new issue of securities with no established trading market. We do not intend to apply for listing of the Bonds on any national securities exchange or for quotation of the Bonds on any automated dealer quotation system. The initial purchasers have advised us that they presently intend to make a market in the Bonds after completion of this offering. However, they are under no obligation to do so and may discontinue any market-making activities at any time without any notice.

Price Stabilization and Short Positions

In connection with the offering, the initial purchasers may engage in transactions that stabilize the market price of the Bonds. Such transactions consist of bids or purchases to peg, fix or maintain the price of the Bonds. If the initial purchasers create a short position in the Bonds in connection with the offering, i.e., if they sell more Bonds than are listed on the cover page of this offering memorandum, the initial purchasers may reduce that short position by purchasing Bonds in the open market. Purchases of a security to stabilize the price or to reduce a short position may cause the price of the security to be higher than it might be in the absence of such purchases.

Neither we nor the initial purchasers make any representation or prediction as to the direction or magnitude of any effect that the transactions described above may have on the price of the Bonds. In addition, neither we nor the initial purchasers make any representation that we will engage in these transactions or that these transactions, once commenced, will not be discontinued without notice.

Other Relationships

Some of the initial purchasers and their affiliates have engaged in, and may in the future engage in, investment banking and other commercial dealings in the ordinary course of business with us or our affiliates. They have received, or may in the future receive, customary fees and commissions for these transactions. In addition, affiliates of the initial purchasers are agents and lenders under certain of our and certain of our affiliates' credit agreements.

In addition, in the ordinary course of their business activities, the initial purchasers and their affiliates may make or hold a broad array of investments and actively trade debt and equity securities (or related derivative securities) and financial instruments (including bank loans) for their own account and for the accounts of their customers. Such investments and securities activities may involve securities or instruments of ours or our affiliates. If the initial purchasers or their affiliates have a lending relationship with us, they routinely hedge their credit exposure to us consistent with their customary risk management policies. Typically, the initial purchasers and their affiliates would hedge such exposure by entering into transactions, which consist of either the purchase of credit default swaps or the creation of short positions in our securities, including potentially the Bonds offered hereby. Any such short positions could adversely affect future trading prices of the Bonds offered hereby. The initial purchasers and their affiliates may also make investment recommendations or publish or express independent research views in respect of such securities or financial instruments and may hold, or recommend to clients that they acquire, long and/or short positions in such securities and instruments.

Settlement

We expect that the delivery of the Bonds will be made to investors on or about September 19, 2013, which will be the fifth business day following the date of this offering memorandum (such settlement being referred to as "T + 5"). Under Rule 15c6-1 under the Securities Exchange Act of 1934, trades in the secondary market are required to settle in three business days, unless the parties to any such trade expressly agree otherwise. Accordingly, purchasers who wish to trade Bonds on the date of pricing or the next succeeding business day will be required, by virtue of the fact that the Bonds initially settle in T + 5, to specify an alternate settlement arrangement at the time of any such trade to prevent a failed settlement. Purchasers of the Bonds who wish to trade the Bonds on the date of pricing or the next succeeding business day should consult their advisors.

Selling Restrictions

Notice to Prospective Investors in the European Economic Area

In relation to each Member State of the European Economic Area (each, a "Relevant Member State"), no offer of the Bonds may be made to the public in that Relevant Member State other than:

- A. to any legal entity which is a qualified investor as defined in the Prospectus Directive;
- B. to fewer than 100 or, if the Relevant Member State has implemented the relevant provision of the 2010 PD Amending Directive, 150, natural or legal persons (other than qualified investors as defined in the Prospectus Directive), as permitted under the Prospectus Directive, subject to obtaining the prior consent of the representatives; or
- C. in any other circumstances falling within Article 3(2) of the Prospectus Directive,
provided that no such offer of the Bonds shall require the Company or the representatives to publish a prospectus pursuant to Article 3 of the Prospectus Directive or supplement a prospectus pursuant to Article 16 of the Prospectus Directive.

Each person in a Relevant Member State who initially acquires any Bonds or to whom any offer is made will be deemed to have represented, acknowledged and agreed that it is a "qualified investor" within the meaning of the law in that Relevant Member State implementing Article 2(1)(e) of the Prospectus Directive. In the case of any Bonds being offered to a financial intermediary as that term is used in Article 3(2) of the Prospectus Directive, each such financial intermediary will be deemed to have represented, acknowledged and agreed that the Bonds acquired by it in the offer have not been acquired on a non-discretionary basis on behalf of, nor have they been acquired with a view to their offer or resale to, persons in circumstances which may give rise to an offer of any Bonds to the public other than their offer or resale in a Relevant Member State to qualified investors as so defined or in circumstances in which the prior consent of the representatives has been obtained to each such proposed offer or resale.

The Company, the representatives and their affiliates will rely upon the truth and accuracy of the foregoing representations, acknowledgements and agreements.

This offering memorandum has been prepared on the basis that any offer of the Bonds in any Relevant Member State will be made pursuant to an exemption under the Prospectus Directive from the requirement to publish a prospectus for offers of the Bonds. Accordingly any person making or intending to make an offer in that Relevant Member State of the Bonds which are the subject of the offering contemplated in this offering memorandum may only do so in circumstances in which no obligation arises for the Company or any of the initial purchasers to publish a prospectus pursuant to Article 3 of the Prospectus Directive in relation to such offer. Neither the Company nor the initial purchasers have authorized, nor do they authorize, the making of any offer of the Bonds in circumstances in which an obligation arises for the Company or the initial purchasers to publish a prospectus for such offer.

For the purpose of the above provisions, the expression "an offer to the public" in relation to any of the Bonds in any Relevant Member State means the communication in any form and by any means of sufficient information on the terms of the offer and the Bonds to be offered so as to enable an investor to decide to purchase or subscribe the Bonds, as the same may be varied in the Relevant Member State by any measure implementing the Prospectus Directive in the Relevant Member State and the expression "Prospectus Directive" means Directive 2003/71/EC (including the 2010 PD Amending Directive, to the extent implemented in the Relevant Member States) and includes any relevant implementing measure in the Relevant Member State and the expression "2010 PD Amending Directive" means Directive 2010/73/EU.

Notice to Prospective Investors in the United Kingdom

In addition, in the United Kingdom, this document is being distributed only to, and is directed only at, and any offer subsequently made may only be directed at persons who are "qualified investors" (as defined in the Prospectus Directive) (i) who have professional experience in matters relating to investments falling within Article 19 (5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005, as amended (the "Order") and/or (ii) who are high net worth companies (or persons to whom it may otherwise be lawfully communicated) falling within Article 49(2)(a) to (d) of the Order (all such persons together being referred to as "relevant persons"). This document must not be acted on or relied on in the United Kingdom by persons who are not relevant persons. In the United Kingdom, any investment or investment activity to which this document relates is only available to, and will be engaged in with, relevant persons.

TRANSFER RESTRICTIONS

The Bonds have not been registered under the Securities Act and may not be offered or sold within the United States or to, or for the account or benefit of, any U.S. person (as such terms are defined under the Securities Act) except pursuant to an exemption from, or in a transaction not subject to, the registration requirements of the Securities Act. Accordingly, the Bonds are being offered hereby only to qualified institutional buyers ("QIBs") in reliance on the exemption from the registration requirements of the Securities Act provided by Rule 144A under the Securities Act and outside the United States to persons other than U.S. persons in reliance on Regulation S under the Securities Act.

Each purchaser of the Bonds, by its acceptance thereof, will be deemed to have acknowledged, represented to and agreed with us and the initial purchasers as follows:

- (1) It understands and acknowledges that the Bonds have not been registered under the Securities Act or any other applicable securities law, the Bonds are being offered for resale in transactions not requiring registration under the Securities Act or any other securities laws, including sales pursuant to Rule 144A under the Securities Act, and none of the Bonds may be offered, sold or otherwise transferred except in compliance with the registration requirements of the Securities Act or any other applicable securities law, pursuant to an exemption therefrom or in a transaction not subject thereto and in each case in compliance with the conditions for transfer set forth in paragraph (5) below.
- (2) It acknowledges that this offering memorandum relates to an offering that is exempt from registration under the Securities Act and does not comply in important respects with SEC rules that would apply to an offering document relating to a public offering of securities.
- (3) It is either:
 - (a) QIB and is aware that any sale of the Bonds to it will be made in reliance on Rule 144A and such acquisition will be for its own account or for the account of another QIB; or
 - (b) an institution that, at the time the buy order for the Bonds is originated, was outside the United States and was not a U.S. person (and was not purchasing for the account or benefit of a U.S. person) within the meaning of Regulation S under the Securities Act (an "Initial Foreign Purchaser").
- (4) It acknowledges that none of us or the initial purchasers or any person representing us or the initial purchasers have made any representation to it with respect to us or the offering or sale of any Bonds, other than the information contained in or incorporated by reference into this offering memorandum or in an additional written communication prepared by us or on our behalf, which offering memorandum and additional written communications, if any, have been delivered to it. Accordingly, it acknowledges that no representation or warranty is made by the initial purchasers as to the accuracy or completeness of such materials. It has had access to such financial and other information as it has deemed necessary in connection with its decision to purchase any of the Bonds, including an opportunity to ask questions of and request information from us and the initial purchasers, and it has received and reviewed all information that was requested.
- (5) If it is an Initial Foreign Purchaser, it understands that (a) during the distribution compliance period, which is the 40-day period following the issue date for the Bonds (the "distribution compliance period"), beneficial interests in the Regulation S global security may be transferred only on receipt by the trustee of a certification on behalf of the beneficial owner that the transferee is either (i) not a U.S. person under Regulation S or (ii) a U.S. person who purchased the debt securities in a transaction that did not require registration under the Securities Act.
- (6) It is purchasing the Bonds for its own account, or for one or more investor accounts for which it is acting as a fiduciary or agent, in each case for investment, and not with a view to, or for offer or sale in connection with, any distribution thereof in violation of the Securities Act, subject to any requirement of law that the disposition of its property or the property of such investor account or accounts be at all times within its or their control and subject to its or their ability to resell such Bonds pursuant to Rule 144A, Regulation S or any exemption from registration available under the Securities Act. It agrees on its own behalf and on behalf of any investor account for which it is purchasing the Bonds, and each subsequent holder of the Bonds by its acceptance thereof will agree, to offer, sell or otherwise transfer such Bonds prior to the date which is six months after the last to occur of the date of the original issue of the Bonds, the issue date of any additional Bonds and the last date on which we or any of our affiliates was the owner of such Bonds (the "Resale Restriction Termination Date") only (a) to us or any of our subsidiaries, (b) pursuant to a registration statement which has been declared effective under

the Securities Act, (c) for so long as the Bonds are eligible for resale pursuant to Rule 144A, to a person it reasonably believes is a QIB that purchases for its own account or for the account of a QIB to whom notice is given that the transfer is being made in reliance on Rule 144A, (d) pursuant to offers and sales to non-U.S. persons that occur outside the United States within the meaning of Regulation S under the Securities Act or (e) pursuant to any other available exemption from the registration requirements of the Securities Act, subject in each of the foregoing cases to any requirement of law that the disposition of its property or the property of such investor account or accounts be at all times within its or their control and to compliance with any applicable state securities laws.

Each purchaser acknowledges that we and the Trustee reserve the right prior to any offer, sale or other transfer of the Bonds pursuant to clause (d) prior to the end of the distribution compliance period or pursuant to clause (e) prior to the Resale Restriction Termination Date to require the delivery of an opinion of counsel, certifications and/or other information satisfactory to us and the Trustee. Each purchaser acknowledges that each certificate representing a Bond will contain a legend substantially to the following effect:

"THE SECURITY (OR ITS PREDECESSOR) EVIDENCED HEREBY WAS ORIGINALLY ISSUED IN A TRANSACTION EXEMPT FROM REGISTRATION UNDER SECTION 5 OF THE UNITED STATES SECURITIES ACT OF 1933, AS AMENDED (THE "SECURITIES ACT"), AND THE SECURITY EVIDENCED HEREBY MAY NOT BE OFFERED, SOLD OR OTHERWISE TRANSFERRED IN THE ABSENCE OF SUCH REGISTRATION OR AN APPLICABLE EXEMPTION THEREFROM. EACH PURCHASER OF THE SECURITY EVIDENCED HEREBY IS HEREBY NOTIFIED THAT THE SELLER MAY BE RELYING ON THE EXEMPTION FROM THE PROVISIONS OF SECTION 5 OF THE SECURITIES ACT PROVIDED BY RULE 144A THEREUNDER. THE HOLDER OF THE SECURITY EVIDENCED HEREBY AGREES FOR THE BENEFIT OF THE COMPANY THAT (A) SUCH SECURITY MAY BE RESOLD, PLEDGED OR OTHERWISE TRANSFERRED, ONLY (1)(a) INSIDE THE UNITED STATES TO A PERSON WHO THE SELLER REASONABLY BELIEVES IS A QUALIFIED INSTITUTIONAL BUYER (AS DEFINED IN RULE 144A UNDER THE SECURITIES ACT) PURCHASING FOR ITS OWN ACCOUNT OR FOR THE ACCOUNT OF A QUALIFIED INSTITUTIONAL BUYER IN A TRANSACTION MEETING THE REQUIREMENTS OF RULE 144A UNDER THE SECURITIES ACT, (b) OUTSIDE THE UNITED STATES TO A FOREIGN PERSON IN A TRANSACTION MEETING THE REQUIREMENTS OF RULE 903 OR RULE 904 OF REGULATION S UNDER THE SECURITIES ACT, (c) PURSUANT TO AN EXEMPTION FROM REGISTRATION UNDER THE SECURITIES ACT PROVIDED BY RULE 144 THEREUNDER (IF APPLICABLE) OR (d) IN ACCORDANCE WITH ANOTHER EXEMPTION FROM THE REGISTRATION REQUIREMENTS OF THE SECURITIES ACT (AND BASED UPON AN OPINION OF COUNSEL ACCEPTABLE TO THE COMPANY IF THE COMPANY SO REQUESTS), (2) TO THE COMPANY OR (3) PURSUANT TO AN EFFECTIVE REGISTRATION STATEMENT AND, IN EACH CASE, IN ACCORDANCE WITH ANY APPLICABLE SECURITIES LAWS OF ANY STATE OF THE UNITED STATES OR ANY OTHER APPLICABLE JURISDICTION AND (B) THE HOLDER WILL, AND EACH SUBSEQUENT HOLDER IS REQUIRED TO, NOTIFY ANY PURCHASER OF THE SECURITY EVIDENCED HEREBY OF THE RESALE RESTRICTIONS SET FORTH IN CLAUSE (A) ABOVE. NO REPRESENTATION CAN BE MADE AS TO THE AVAILABILITY OF THE EXEMPTION PROVIDED BY RULE 144 FOR RESALE OF THE SECURITY EVIDENCED HEREBY."

- (7) If it is (a) a purchaser in a sale that occurs outside the United States within the meaning of Regulation S under the Securities Act or (b) a "distributor," "dealer" or person "receiving a selling concession, fee or other remuneration" in respect of Bonds sold, prior to the expiration of the distribution compliance period, it acknowledges that until the expiration of such "distribution compliance period" any offer or sale of the Bonds shall not be made by it to a U.S. person or for the account or benefit of a U.S. person within the meaning of Rule 902(k) of the Securities Act.
- (8) If it is an Initial Foreign Purchaser, it acknowledges that, until the expiration of the distribution compliance period, it may not, directly or indirectly, refer, resell, pledge or otherwise transfer a Bond or any interest therein except to a person who certifies in writing to the applicable transfer agent that such transfer satisfies, as

applicable, the requirements of the legends described above and that the Bonds will not be accepted for registration of any transfer prior to the end of the distribution compliance period unless the transferee has first complied with the certification requirements described in this paragraph.

- (9) It acknowledges that we, the initial purchasers and others will rely on the truth and accuracy of the foregoing acknowledgments, representations, warranties and agreements and agrees that if any of the acknowledgments, representations, warranties and agreements deemed to have been made by its purchase of the Bonds are no longer accurate, it shall promptly notify us and the initial purchasers. If it is acquiring any Bonds as a fiduciary or agent for one or more investor accounts, it represents that it has sole investment discretion with respect to each such investor account and that it has full power to make the foregoing acknowledgments, representations and agreements on behalf of each such investor account.
- (10) Each purchaser and transferee of a Bond will be deemed to have represented by its purchase and holding of the Bond that (a) its purchase and holding of the Bond is not made on behalf of or with "plan assets" of any plan subject to Title I of ERISA, Section 4975 of the Code or any similar law or (b) its purchase and holding of the Bond will not result in a non-exempt prohibited transaction under Section 406 of ERISA, Section 4975 of the Code or any similar law.

LEGAL MATTERS

The validity of the Bonds is being passed upon for us by Michael S. Mizell, Senior Vice President and General Counsel of The Dayton Power and Light Company, and by Skadden, Arps, Slate, Meagher & Flom LLP, New York, New York. Certain matters under Ohio law will be passed upon by Porter Wright Morris and Arthur, LLP. The initial purchasers are being advised by Shearman & Sterling LLP, New York, New York.

INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRMS

Our financial statements and schedule as of December 31, 2012 and for the year ended December 31, 2012, incorporated into this offering memorandum by reference to the Annual Report on Form 10-K for the year ended December 31, 2012, have been audited by Ernst & Young LLP, independent registered public accounting firm, as stated in their report appearing therein.

Our financial statements and schedule as of December 31, 2011, and for each of the years in the two-year period ended December 31, 2011, incorporated into this offering memorandum by reference to the Annual Report on Form 10-K for the year ended December 31, 2012, have been audited by KPMG LLP, independent registered public accounting firm, as stated in their report appearing therein.



The Dayton Power and Light Company

**FIRST MORTGAGE BONDS
1.875% SERIES DUE 2016**

**BofA Merrill Lynch
Morgan Stanley
Fifth Third Securities, Inc.
PNC Capital Markets LLC
US Bancorp
BMO Capital Markets
Huntington Investment Company
Regions Securities LLC**
