

**BEFORE THE
PUBLIC UTILITIES COMMISSION OF OHIO**

THE DAYTON POWER AND LIGHT COMPANY

CASE NO. 20-1651-EL-AIR

CASE NO. 20-1652-EL-AAM

CASE NO. 20-1653-EL-ATA

2020 DISTRIBUTION BASE RATE CASE

**BOOK I – APPLICATION AND SUPPLEMENTAL
VOLUME 3 OF 11**

Dayton Power and Light Company
DP&L Case No. 20-1651-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, (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	4	Appendix A, Chapter II, (C)(1)	Supplemental	The most recent Federal Energy Regulatory Commission's ("FERC") audit report.
1	4	Appendix A, Chapter II, (C)(2)	Supplemental	Prospectuses of current stock and/or bond offering of the applicant, and/or of parent company.
1	5-8	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	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	9	Appendix A, Chapter II, (C)(5)	Supplemental	Working papers supporting the schedules.
1	9	Appendix A, Chapter II, (C)(6)	Supplemental	Worksheet showing monthly test year data by FERC account.
1	9	Appendix A, Chapter II, (C)(7)	Supplemental	CWIP included in the prior case.
1	9	Appendix A, Chapter II, (C)(8)	Supplemental	Copy of latest certificate of valuation from department of taxation.
1	9	Appendix A, Chapter II, (C)(9)	Supplemental	Monthly sales for the test year by rate schedule classification and/or customer classes.
1	9	Appendix A, Chapter II, (C)(10)	Supplemental	Written summary explaining the forecasting method used by the utility as related to test year data.
1	9	Appendix A, Chapter II, (C)(11)	Supplemental	Explanation of computation of materials and supplies.
1	10	Appendix A, Chapter II, (C)(12)	Supplemental	Depreciation expense related to specific plant accounts.
1	10	Appendix A, Chapter II, (C)(13)	Supplemental	Federal income tax information.
1	10	Appendix A, Chapter II, (C)(14)	Supplemental	Other rate base items and detailed information.
1	10	Appendix A, Chapter II, (C)(15)	Supplemental	Copy of all advertisements in the test year.
1	10	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	10	Appendix A, Chapter II, (C)(17)	Supplemental	Depreciation study showing depreciation reserves allocated to accounts.
1	10	Appendix A, Chapter II, (C)(18)	Supplemental	Depreciation study.
1	11	Appendix A, Chapter II, (C)(19)	Supplemental	Depreciation reserve data from the last date certain to the date certain in the current case.
1	11	Appendix A, Chapter II, (C)(20)	Supplemental	Construction project details for projects that are at least seventy-five percent complete.
1	11	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	11	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. 20-1651-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. 20-1651-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-3.26	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. 20-1651-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	2	Appendix A, Chapter II, Section E(B)(2)(a)	E-2	Current Tariff Schedules
2	3	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

Functional Area:**Technical Operations and Engineering****SFR Reference:****(B)(9)(a)(ii) Operations and Maintenance****Policy and Goal Setting:**

DP&L's Technical Operations and Engineering policies have evolved to be responsive to and meet federal, state and local regulations and policies. DP&L's policies are developed by DP&L's management team under the guidance of 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 DP&L's regulating entities.

The first priority of Technical Operations and Engineering is to ensure the safety of all DP&L employees, contractors and the public. Technical Operations and Engineering takes this priority very seriously and incorporates safety into all aspects of operations. The safety program focuses on getting everyone actively involved in safety in order to increase safety awareness and create an injury-free workplace.

Technical Operations and Engineering goals are set annually in support of company and corporate goals. Goals include targets for safety, compliance, environmental, reliability, and cost management. Each of these goals comes with specific objectives and schedules to ensure completion. DP&L's Technical Operations and Engineering organization is committed to meeting or exceeding applicable local, state and federal regulatory requirements.

Strategic and Long-Range Planning:

Planning in Technical Operations and Engineering 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' energy needs.

Technical Operations and Engineering annually provides technical project guidance to the capital investment plan that projects the needs for the coming 10-year period. Plans typically include transmission and substation projects which relate to known areas of customer growth or to address reliability concerns, substation modernization and other planned system expansions and upgrades. In addition to operational needs, planning considers budget allowances and staffing needs.

Organizational Structure and Responsibilities:

Technical Operations and Engineering consist of 103 employees and is led by the Director of Technical Operations and Engineering. This area maintains responsibility for the following utility activities:

Substation Maintenance and Construction is predominantly operated out of eight districts within DP&L's service area and is responsible for the construction, maintenance, and emergency restoration related to substations and other technical areas of the transmission and distribution system. Two substation technicians report to each of the eight districts to assure rapid response to equipment alarms, outages and system emergencies. Activities include:

- 1) Provide maintenance and emergency restorations operations to 155 substations
- 2) Perform routine maintenance activities such as breaker maintenance, load tap changer maintenance, bushing change outs, substation fence inspections, infrared inspections and monthly substation inspections. A listing of Substation Operations maintenance policies is included as Technical Operations and Engineering – Exhibit 2
- 3) Manage construction activities related to additional new substations and major renovation or replacements at existing substations
- 4) Ensure construction projects are completed on time, on budget and in accordance with DP&L standards
- 5) Respond to substation equipment outages, alarms and complete switching within substations or on the line as directed by System Operating

Substation Engineering is responsible for engineering substation projects and the development of substation technical resources for system design and operations. Substation Engineering performs the following specific duties:

- 1) Engineer substation projects in accordance with DP&L standards. A listing of DP&L's engineering standards is included as Technical Operations and Engineering – Exhibit 3
- 2) Create construction drawings and associated bills of material for various projects
- 3) Specify and obtain materials/equipment specific to a project
- 4) Support siting and permitting processes
- 5) Develop equipment specification and standards
- 6) Develop project scopes and estimates
- 7) Manage substation projects
- 8) Provide construction support
- 9) Setup and closeout projects in the financial system
- 10) Maintain engineering prints and schematics associated with substations and equipment
- 11) Research and implement new technologies
- 12) Support NERC compliance
- 13) Provide technical support during emergency response situations

Relay Engineering is responsible for the design of the protective relaying systems, used on the electric system to protect employees, equipment and the public. Relay Engineering performs the following specific duties:

- 1) Specify relays and associated communications systems
- 2) Design protective relay systems and work with Substation Engineering in the development of project drawings
- 3) Specify settings for protective relays
- 4) Maintain engineering records associated with relays and protective systems
- 5) Support field personnel in the installation and troubleshooting of relay systems
- 6) Manage relay projects
- 7) Support electrical event investigations
- 8) Coordinate protective systems between the grid and generators as well as with other interconnected electric utilities and large customers
- 9) Research and implement new technologies
- 10) Support NERC compliance
- 11) Provide technical support during emergency response situations

Test Department is operated centrally from the Dayton Service Building and is responsible for the analytical testing of substation class equipment and distribution line equipment as well as maintaining all protective relays. Activities include:

- 1) Test substation equipment, line capacitors, reclosers, line regulators and network protectors
- 2) Conduct relay calibration, line carrier testing and breaker time travel testing
- 3) Commission new substation equipment or relay systems to ensure proper operation and communications prior to the equipment being energized
- 4) Investigate voltage and power quality concerns and work with customers to address their concerns
- 5) Locate underground cable faults

AC Network is operated centrally out of the Dayton Service Building and is responsible for the construction, maintenance, and emergency restoration related to the underground duct and manhole system and the downtown network. Activities include:

- 1) Ensure the reliable operation and maintenance of the downtown Dayton and City of Troy network systems as well as the electrical infrastructure serving the Dayton International Airport
- 2) Repair and maintain substation riser cables
- 3) Provide all maintenance and emergency services when confined space entry is required. Confined space entry is primarily needed when working on the manhole systems located in downtown Dayton, downtown Troy, the Dayton International Airport and WPAFB
- 4) Manage a portion of the underground inspection program which includes periodic inspections of the network and vaults
- 5) Support restoration efforts in substations, switching and underground locating

WPAFB Operations is responsible for managing DP&L's compliance with the Wright Patterson Air Force Base (WPAFB) privatization contract. The contract includes maintaining the transmission and distribution system which is located beyond WPAFB's utility meters. Activities include:

- 1) Regular customer contact related to system maintenance, construction and operational activities
- 2) Complete all contractually required reporting, pricing and billing
- 3) Coordinate DP&L's activities with base personnel
- 4) Communication and technical support during emergency response situations
- 5) Project management for new construction, system expansion and renewal and replacement activities

Design Engineering provides engineering design and technical support for all new customer construction as well as maintenance related projects designed to improve or upgrade the reliability of DP&L's electrical distribution system. Activities include:

- 1) Provide design and technical support for all new customer construction projects
- 2) Provide design and technical support for all maintenance related projects intended to improve or upgrade the reliability of DP&L's distribution system
- 3) Provide design and technical support for all customer requested relocations or upgrades
- 4) Management of the pole attachment process
- 5) Engineering analysis of field hazards

Transmission Engineering is responsible for transmission line projects and the development of technical resources with an in-depth understanding of transmission system design and operations. Activities include:

- 1) Create construction drawings and associated bills of material for various projects
- 2) Specify and obtain materials/equipment specific to a project
- 3) Develop siting and permitting processes
- 4) Support equipment specification and standards processes
- 5) Develop project scopes and estimates
- 6) Maintain and update engineering drawings associated with transmission lines and equipment
- 7) Perform line encroachment investigations

The organizational chart for Technical Operations & Engineering is included as Technical Operations and Engineering – Exhibit 1.

Decision-Making and Control:

Technical Operations and Engineering 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 appropriately raised to proper level of authority as required by DP&L's policies. Overall responsibility for all decisions is that of the Senior Director of Customer Operations.

Performance against the Customer Operations goals is monitored and reported on a continuous basis, which includes monitoring of safety, reliability, 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.

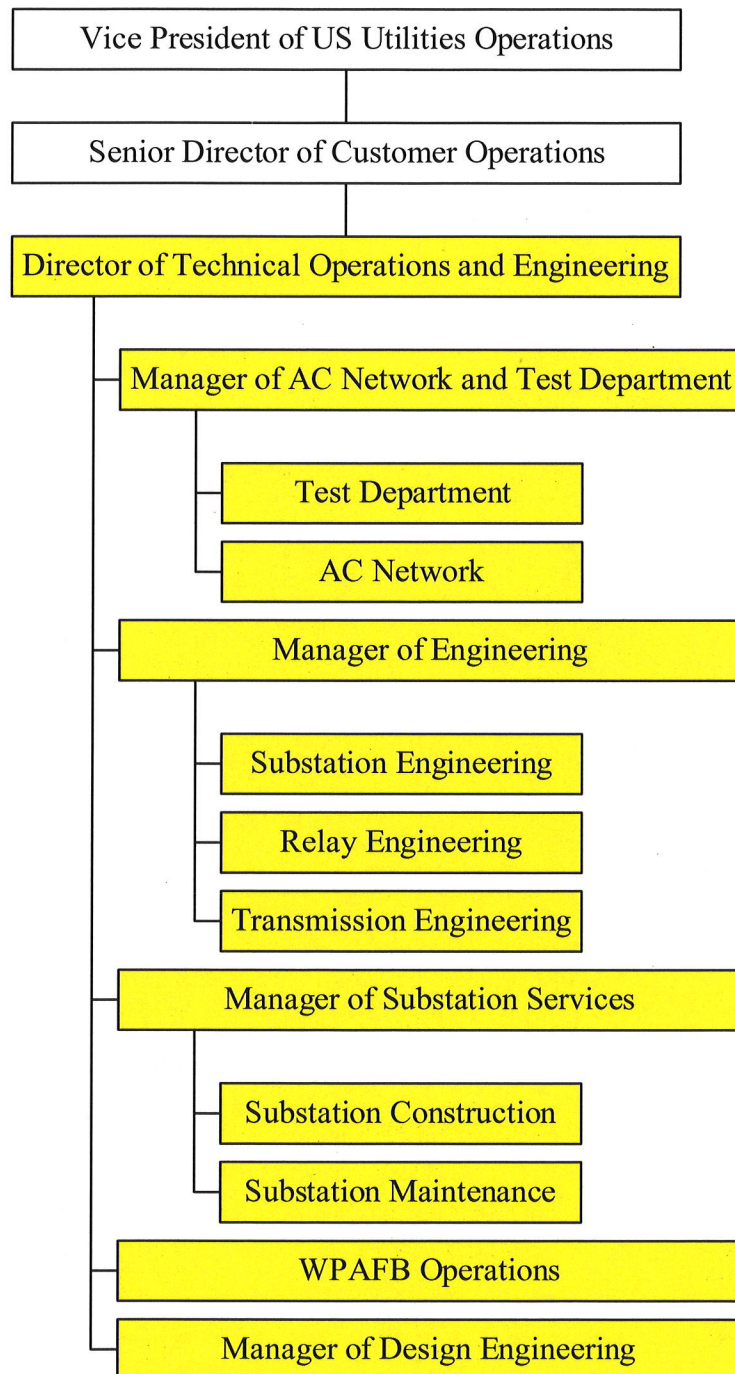
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including; phone calls, conference calls, scheduled meetings and e-mail. Internal communications typically correspond to scheduling projects, maintenance, troubleshooting and in the support of other functional areas within DP&L. These communications include providing information to areas such as Engineering, Dispatch Operations, Customer Service, Community Relations, Finance, and Regulatory.

External communications are accomplished through a variety of communication channels including; phone calls, meetings, and e-mail. Personnel within Technical Operations and Engineering will communicate directly with communities or larger customers when technical issues arise. Communications typically involve a variety of topics including; outage restoration, technical issue resolution, construction projects, and maintenance activities.

Technical Operations and Engineering – Exhibit 1

Organizational Chart for Technical Operations and Engineering



Technical Operations and Engineering – Exhibit 2

List of Customer Operations Procedures for Electric Operations – Substation Maintenance

- Purpose, Objective and Results
- Maintenance Responsibilities
- Important Contacts
- S/O Prints
- Master Capabilities Listing
- Switching Order Set-Ups
- Substation Inspections
- Thermographic Imaging
- Spill Prevention, Control and Counter Measures Plan
- Computerized Maintenance Management System
- RCM Strategy / Batteries
- RCM Strategy / Transformer
- RCM Strategy / Breaker
- RCM strategy / Voltage Regulators
- Relay Calibration Test and Maintenance Schedule
- PUCO Electric Service & Safety Standards
- Safety
- Transmission Protection System Maintenance and Testing

Technical Operations and Engineering – Exhibit 3

List of DP&L's Engineering Standards

- Power Plant, Substation and Telecommunication Batteries Procedures Manual
- Substation Standards
 - Alarms
 - Ampacities
 - Bus Design
 - Bushings
 - Cable
 - Capacitor Installations
 - Carrier
 - Circuits
 - Circuit Breakers
 - Electrical Clearances
 - Connectors and Dies
 - Customer Installations
 - Drawings
 - Filing Procedures
 - Fire Protection
 - Foundations
 - Function Numbers
 - Fusing
 - Grounding
 - Indicating Lights
 - Insulators
 - Interlocks
 - Lightning Protection and Coordination
 - Metering
 - Mobile Substation
 - Motor Operations
 - Phasing
 - Polarity
 - Potential Throwover
 - Relaying
 - Specifications
 - Station Power Auxiliaries
 - Switchboard
 - Switches
 - Transformers
 - Vendors Lists
 - Wire Identification

Functional Area:
Telecommunications

Policy and Goal Setting:

Policies are developed by DP&L's management under the guidance of 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 DP&L's regulating entities.

The first priority of all DP&L areas is to ensure the safety of all DP&L employees, contractors and the public. Telecommunications employees attend monthly safety meetings which cover topics relevant to work activity and allow employees to share concerns and experiences. Further, employees are properly outfitted with appropriate personal protective equipment if needed in their duties.

Telecommunication's goals are set annually in support of company and corporate goals. Goals include targets for safety, compliance, timeliness, and budgets.

Strategic and Long-Range Planning:

Planning in Telecommunications 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.

Annually the Telecommunications department plans its resources and prioritizes projects to meet regulatory requirements, meet operational and customers' needs to establish reliable transmission and distribution communication systems. Telecommunications equipment and system upgrades are reviewed regularly to ensure that the necessary components and tools in place to meet the needs of our transmission and distribution system, employees, customers and all regulatory requirements. Long-term planning for this department includes initiatives to modernize technology systems, cyber security compliance, network infrastructure, refine business processes, and to utilize technologies to work safely and efficiently.

Organizational Structure and Responsibilities:

Telecommunications consists of a manager and 7 employees who report to the Director of Metering and Operational Technology. This area maintains responsibility for the following utility activities:

- 1) Design, construct, and ensure reliable performance for the DP&L transmission and distribution communication and telecom assets used to manage the power system. These assets are critical for electrical grid operations

- 2) Support a wide variety of hardware, software, T&D operations, networking systems, firewalls, security, radio and microwave systems, remote field devices, and other technology involving new and existing legacy systems, along with supporting the AES Digital Strategy
- 3) Maintain systems that operate 24x7 and are used by T&D field, engineering, planning, reporting and dispatch staff
- 4) Ensure substation communication is secure and oversee configuring firewalls, routing and switching to maximize network efficiency and all security and compliance guidelines
- 5) Strategic planning for technological innovation in telephony, serves as a principal advisor to the business on new developments in telecommunications and advise on how they might be integrated into the current, and future, telephony environment.
- 6) Research federal, state and local laws, rules, regulations, ordinances, policies and procedures to ensure compliance and client agencies to ensure systems are compliant with all regulatory parameters.

The organizational chart for Telecommunications is included as Telecommunications – Exhibit 1.

Decision-Making and Control:

Telecommunication's 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 appropriately raised to the proper level of authority as required by DP&L's policies. Overall responsibility for all decisions is that of the Vice President of US Utilities Operations.

Performance against the Customer Operations goals are monitored and reported on a continuous basis, which includes monitoring of safety, reliability, 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 phone calls, conference calls and e-mail. Internal communications typically include providing information and supporting field operations and typically involve areas such as Substations, NERC Compliance, Cyber Security, Financial Planning and Analysis, Human Resources and System Operating.

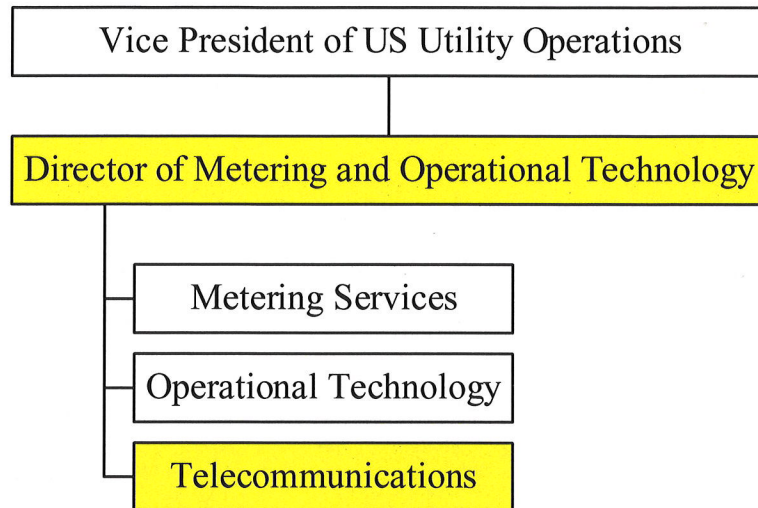
External communications are accomplished through a variety of communication channels including phone calls, meetings, and e-mail. Telecommunications employees will communicate directly with communities, customers, other utilities and vendors as needed. Communications typically involve a variety of topics including engineering activities, material specification and

procurement, operation support, technical issue resolution, construction projects, and maintenance activities.

Employees also attend various meetings with other electric utilities, associations and organizations as delegates or committee members. They conduct joint studies, coordinate projects and discuss issues common to the electric utility industry. They also work with local, state and federal agencies to furnish information as requested.

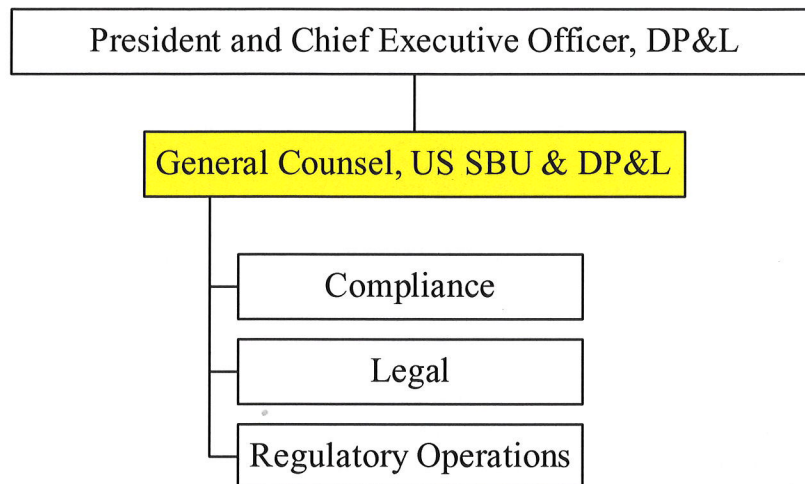
Telecommunications – Exhibit 1

Organizational Chart for Telecommunications



Legal

Legal has overall responsibility for all DP&L legal, regulatory and compliance activities. The Legal functions are described in detail in the following sections.



Functional Area:
Claims Administration

SFR Reference
(B)(9)(c)(i) Legal

Policy and Goal Setting:

DP&L Claims Administration policy is to manage DP&L's Payable Claims, Fleet Claims, Collectable Claims and provide litigation support where needed. DP&L Claims performs these functions in accordance with the protocols developed and maintained in DP&L's tariff.

Strategic and Long-Range Planning:

Strategic planning in Claims Administration supports DP&L's goal of delivering safe reliable electric service, both now and in the future, by responding to and resolving claim issues in a professionally courteous and timely manner. Planning includes continued education for staff personnel to stay abreast of and anticipate changes in the industry.

Organizational Structure and Responsibilities:

Claims Administration consists of the Supervisor of Claims Administration and one dedicated contract worker. This area is responsible for managing the following utility activities:

Payable Claims resolves claims made against the Company for damages that result from the daily operation of an electrical utility

- 1) Investigate claims submitted to the Company by obtaining information from the customer, making field inspections, and contacting responding crews for circumstances and necessary work
- 2) Discuss claim with involved parties, including; customer, attorney, insurer, Public Utilities Commission of Ohio (PUCO), Ohio Consumers' Counsel (OCC) and other consumer agents
- 3) Resolve the claim with the customer

Collectable Claims resolves claims made by the Company for third party damage to its facilities and equipment

- 1) Investigate damages to Company facilities, obtain Company and civil records in support of billing, and prepare billing documents
- 2) Defend, negotiate, and resolve claims with individuals, contractors, and insurance company representatives

Personal Injury Claims & Litigation Support investigates major accidents involving bodily injury and/or significant property damage

- 1) Investigate personal injury or significant property damage claims which may entail an immediate response. Work the accident scene, including; take photographs, gather facts of the accident, gather statements, preserve evidence, and work with field crews and civil authorities
- 2) Assist with activities in support of litigation, gather pertinent records, support Company and outside counsel, testify and develop exhibits as required

Vehicle Fleet Claims coordinates and monitors vehicle fleet claims activity handled by a third-party administrator

- 1) Gather information concerning vehicle fleet traffic accidents, ascertain liability and initiate a damage claim or submit the claim to external fleet adjusters
- 2) Monitor and provide support of outside adjustment agency

The organizational chart for Claims Administration is included as Claims Administration – Exhibit 1.

Decision-Making and Control:

Claims Administration decision-making and control is achieved by individuals in the department 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 appropriately raised to proper level of authority as required by DP&L's policies. Overall responsibility for all decisions is that of an Assistant General Counsel. Control of monetary activities is overseen by the accounting department while complying with the Sarbanes-Oxley Act.

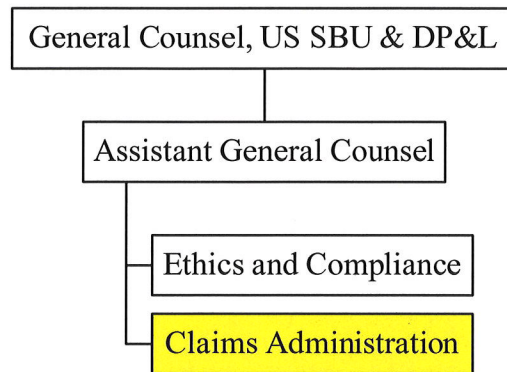
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including; telephone calls, conference calls, company mail, e-mails, and direct meetings. Internal communications typically correspond to supporting the operations of other functional areas of DP&L and typically include Legal, Security, Power Production, Real Estate Services, Line Clearance, Electrical Test, Electric Meter, Customer Service, Central Dispatch Operations, System Operating, Accounting, Services, Line Operations, Substation Services, and Engineering.

External communications are accomplished through a variety of communication channels including; telephone calls, U.S. postal mail, e-mails, and direct meetings with customers, attorneys, insurance agents, outside experts, company contractors, police and fire personnel, and government officials connected to various government agencies.

Claims Administration – Exhibit 1

Organizational chart for Claims Administration



Functional Area:**Ethics and Compliance****SFR Reference****(B)(9)(e)(i) Legal****Policy and Goal Setting:**

The objectives of Ethics and Compliance are to provide services and expertise to support DP&L values and to enable its compliance mechanisms and governance processes to function properly. To accomplish this objective, the Ethics and Compliance Department:

- 1) Assist management in the assessment of ethics matters, compliance issues and related business risks and in the identification of cost beneficial actions to mitigate risks, including potential fraud, to acceptable levels
- 2) Assist management in evaluating whether DP&L's strategy, objectives and goals will be met ethically and effectively
- 3) Interact with various DP&L governance groups as required
- 4) Conduct selected special investigations, reviews, and consulting projects at the request of management, as appropriate
- 5) Follow-up on outstanding management actions and significant issues to validate that these matters are being resolved appropriately and timely
- 6) Work with management to take reasonable steps to respond to inappropriate conduct and to prevent further similar misconduct.

Strategic and Long-Range Planning:

The strategic plan for the Ethics and Compliance Department, which supports the overall strategic direction of DP&L, is created by the North American Ethics and Compliance Officer in conjunction with the AES Corporations Ethics and Compliance Department.

Organizational Structure and Responsibilities:

Ethics and Compliance at DP&L is led by the North American Ethics and Compliance Officer for the US SBU, who reports to an Assistant General Counsel of the US SBU. This reporting relationship is designed to provide sufficient authority to promote independence and to ensure effective coverage and appropriate action and communication regarding ethics and compliance matters.

Ethics and Compliance is responsible for ensuring that the organization is in compliance with corporate policies as well as select regulations from Federal and State regulatory agencies based on the framework provided by the U.S. Federal Sentencing Guidelines for Organizations. Activities include:

- 1) Assist in the investigation of suspected fraudulent activities within DP&L and report the results to management
- 2) Maintain and administer a rigorous follow-up process to ensure that committed management actions to address issues are properly and timely executed
- 3) Administer the anonymous helpline program in an efficient and effective fashion and in full compliance with applicable laws, requirements, and standards
- 4) Foster an appropriate level of ethics and compliance awareness throughout the organization and with vendors, customers and other key stakeholders as appropriate
- 5) Develop and administer effective training programs associated with ethics and compliance issues or matters
- 6) Help foster a culture of fraud awareness and assist in the development and implementation of anti-fraud programs as appropriate
- 7) Periodically evaluate the design, implementation and effectiveness of DP&L's ethics and compliance program
- 8) Discharge these responsibilities in a manner consistent with the purpose and objectives set forth in the DP&L/AES Code of Business Ethics and DP&L Vision and Mission.

An organizational chart for Ethics and Compliance is included as Ethics and Compliance – Exhibit 1.

Decision-Making and Control:

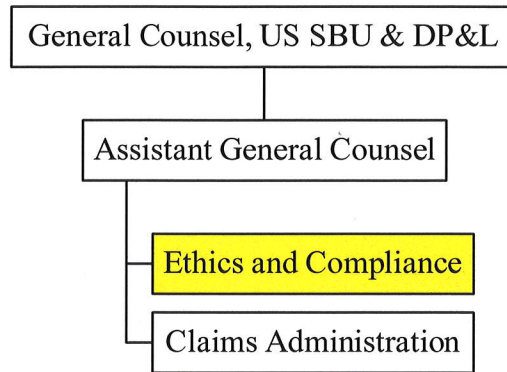
Decision-making authority flows up through the North American Compliance Officer to the Chief Legal Officer.

Internal and External Communications:

Ethics and Compliance personnel, in the performance of their duties and responsibilities, interface frequently with personnel within DP&L through a variety of communication methods; face-to-face, phone, and email correspondence.

Ethics and Compliance – Exhibit 1

Organizational Chart for Ethics and Compliance



Functional Area:**Legal****SFR Reference****(B)(9)(e)(i) Legal****(B)(9)(e)(iv) Records management****Policy and Goal Setting:**

Legal does not establish policy for DP&L or the AES US SBU. Corporate policies are developed by the management of DP&L and the US SBU with support from Legal in an advisory capacity. Legal reviews proposed and existing policies for compliance with applicable state and Federal law, regulations and the AES Code of Conduct.

Department level goals are driven by the goals of the various operating units within DP&L and the US SBU. These team level goals form the foundation for individual goals for each attorney and staff members within Legal. Goals are established on an annual basis early in the calendar year and are monitored and reviewed periodically throughout the year and modified as necessary to align with evolving business objectives. Attorneys and staff members are evaluated at the end of each year based on the modified goals and objectives.

The primary goal of Legal is to serve the operating units comprising the US SBU in a safe, effective and efficient manner. Legal gets involved in DP&L's culture of safety, by attending safety meetings, safety day, and safety walks.

Strategic and Long-Range Planning:

Strategic plans for DP&L and the US SBU are developed by the leadership team of the US SBU under the guidance of AES. Legal serves management in an advisory capacity throughout the planning process by reviewing plans for compliance with applicable state and Federal laws and regulations and also provides any legal assistance necessary to implement plans.

Organizational Structure and Responsibilities:

Legal support for DP&L falls under the control of DP&L's President and Chief Executive Officer and is led by the General Counsel of the US SBU. While no direct reporting relationship exists, frequent consultation and coordination occurs with AES corporate Legal, which is headquartered in Arlington, Virginia. In addition to the General Counsel, Legal is comprised of 8 attorneys that serve the various entities within the US SBU, including DP&L. Additionally, the attorneys are supported by paralegals and administrative staff.

- Legal supports all of the operating units comprising the US SBU and is responsible for providing legal services across all of the functional areas of law that are applicable to the

business operations of the US SBU, including DP&L. Each attorney within Legal focuses his or her practice in one or more of these functional areas:

- State regulatory compliance
 - Federal regulatory compliance
 - Environmental compliance
 - Litigation
 - Ethics and compliance
 - Corporate governance
 - Securities
 - Finance and mergers
 - Acquisitions
 - Labor and employment
 - Commercial contracts
 - Retail
- Attorneys have substantial experience in the area(s) in which they focus and are responsible, under the guidance of the General Counsel, for serving the needs of the business with regard to such area(s)
 - Determine when certain tasks or projects should be delegated to outside counsel
 - Manage outside counsel, the attorney responsible for the applicable functional area is responsible for managing outside counsel
 - Assist outside of their area(s) of emphasis as necessary to meet timelines and objectives
 - Keep current in attorney's area(s) of emphasis through self-study and continuing legal education. Each of the attorneys is required to satisfy the continuing legal education requirements of the state(s) in which he or she is admitted to practice and is responsible for keeping his or her license(s) current
 - Monitor attorney time closely to assure the appropriate allocation of costs across the various legal entities and operating units comprising the US SBU

The organizational chart for Legal is attached as Legal – Exhibit 1.

Decision-Making and Control:

Individuals within the US SBU make decisions within their scope of authority in support of the US SBU's mission and in accordance with US SBU policies and procedures. Decisions are appropriately raised to the proper level of authority as required by US SBU policies. Legal serves in an advisory capacity to the various operating units across the US SBU in support of business decision making. Attorneys are responsible for decisions on legal issues relevant to the functional area(s) in which they focus and have the necessary information and experience to make decisions. The General Counsel has responsibility for decisions made by attorneys and staff within Legal. In the event that work is delegated to outside counsel, the assigning attorney

closely monitors such work and maintains responsibility for any material legal decisions. Outside counsel are selected based on their relevant expertise and cost and, like other suppliers of goods and services to the organization, are required to go through an onboarding process including a thorough due diligence investigation. Invoices submitted by outside counsel are closely reviewed by attorneys for the purpose of ensuring accuracy and monitoring the value of the services relative to the cost. Invoice approval limits are set for each attorney in Legal based upon experience level.

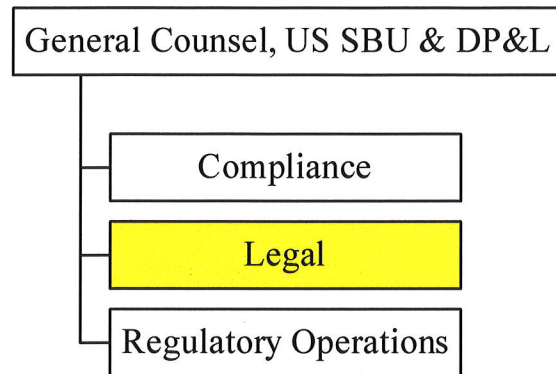
Internal and External Communications:

Legal practices an open door policy with regard to the exchange of communications among team members within the department. Attorneys and legal staff frequently communicate with clients and other individuals at all levels across the US SBU. These communications may be privileged or unprivileged and may consist of phone calls, in person meetings, conference calls, email and other written communications, and legal opinions, which may be formal or informal.

Attorneys frequently correspond with individuals outside of the organization as well, including regulators, financial institutions, customers, suppliers, outside counsel and others. The responsibility for external communications resides with the attorney having the appropriate level of information and experience to make such communications. Legal also coordinates with the communications group regarding external corporate level communications. US SBU policy requires that all press releases issued on behalf of the organization be reviewed and approved by Legal.

Legal – Exhibit 1

Organizational Chart for Legal



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 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 Public Utilities Commission of Ohio (PUCO), the Federal Energy Regulatory Commission (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 General Counsel of the US SBU's objectives, whose goals align with the President and Chief Executive Officer's objectives, which fully support Company and Corporate goals, set by AES's management and board of directors.

Strategic and Long-Range Planning:

Regulatory Operations reflects DP&L's long-term 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. This facilitates AES' mission of "Improving lives by accelerating a safer and greener energy future". DP&L's Financial Planning and Analysis department sets a 10-year long-term financial budget by which actual data is measured and analyzed, including DP&L's long-term capital spending outlook. 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 and Analysis 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:

Regulatory Operations team consists of 3 Rate Analysts and 3 Program Managers who are all ultimately led by the Senior Manager of Regulatory Operations. The Senior Manager of Regulatory Operations reports to the Senior Director of Regulatory who leads both the DP&L and Indianapolis Power and Light Regulatory teams. 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 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 that is consistent with tariff terms and conditions as well as the Ohio Administrative Code. 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: SAP, 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 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) Grid Modernization Plan – Settlement discussions to determine the appropriate level of spending for Smart Grid type capital expenditures for recovery through DP&L's Infrastructure Investment Rider
- 2) FERC Transmission Formula Rate Filing – Filing to update DP&L's FERC Transmission rate from a stated rate to a formula rate, subject to refund based on case outcome

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 AES' overall mission and in accordance with the DP&L policies and procedures. Decisions are appropriately raised to proper level of authority as required by DP&L's policies. Overall responsibility for all Regulatory Operations decisions is that of the General Counsel, US SBU.

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.

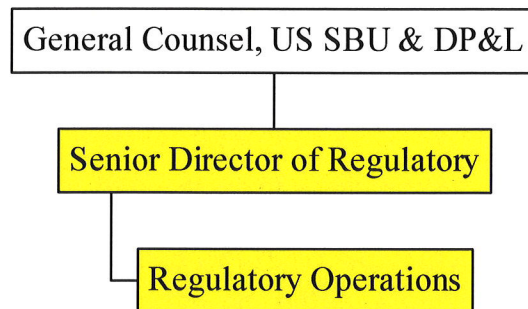
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including; phone calls, conference calls (through Microsoft Teams), 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, conference calls (through Microsoft Teams), 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, website bill calculator and a list of registered CRES Providers.

Regulatory Operations – Exhibit 1

Organizational Chart for Regulatory Operations



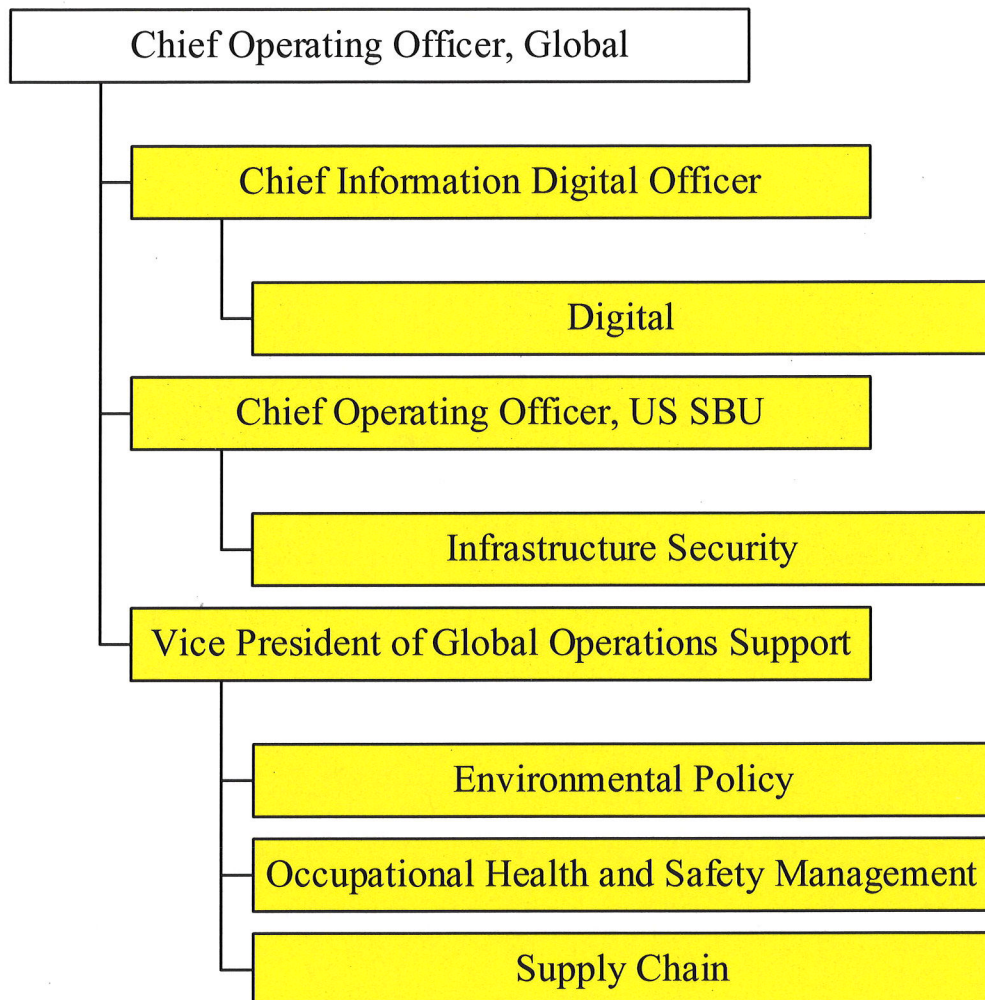
Regulatory Operations – Exhibit 2

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 I Commission Order

Office of the Chief Operating Officer, Global

The Global COO is responsible to provide shared services which benefit DP&L by sharing costs amongst several AES businesses, providing DP&L the services it needs at a reduced cost. The functions provided by Global Chief Operating Officer are described in detail in the following sections.



Functional Area:
Environmental Policy

SFR Reference
(B)(9)(a)(viii) Environmental management

Policy and Goal Setting:

DP&L has adopted the Global AES environmental policy statement that is intended to be responsive to federal, state and local regulations and policies. These guidelines reflect DP&L's commitment to the environment and require DP&L leaders to develop a balanced approach to meeting these guidelines; one that considers all environmental standards and requirements, as well as the needs of all stakeholders (including social and other needs of the local community). All people within the organization are equally responsible to ensure that the Company's activities meet the requirements set forth by all DP&L's regulating entities as well as the Global AES Environmental Policy.

A key part of Environmental Policy's responsibilities is creating policies and training that help to keep people safe. Environmental Policy takes safety into strong consideration in the development of policies and training to make employees aware of the hazards and personal protective equipment needed to ensure safety when dealing with different hazardous conditions.

Global AES establishes annual environmental goals and all AES businesses are expected to achieve these goals. The annual AES goals are designed to drive continued environmental performance improvement across the company and contribute to advancing broader company initiatives of sustainability and environmental stewardship. DP&L also establishes separate annual environmental goals as part of the continuous improvement process. Listings of DP&L's and AES's environmental policies are included as Environmental Policy – Exhibits 2 and 3, respectively.

Strategic and Long-Range Planning:

Strategic and long-range planning is focused on ensuring DP&L can continue to deliver safe, reliable service while maintaining compliance to the changing laws and regulations. Environmental Policy keeps abreast of the environmental, regulatory, and legislative climates and ensures that pending environmental issues and risks are incorporated into the business planning process.

Organizational Structure and Responsibilities:

Environmental Policy is structured under the Vice President Global Operations Support, and consists of 9 employees, including the Director of Environmental Policy. Additionally, at each

AES business there is a local environmental professional who oversees environmental responsibilities, which includes ensuring the business meets the AES Global Environmental Policy goals and any separate DP&L goals.

Environmental Policy maintains responsibility for the following activities:

- 1) Identify and analyze key federal environmental issues that could impact DP&L operations
- 2) Advocate for positive environmental regulatory and legislative outcomes through stakeholder outreach
- 3) Promote environmental stewardship through policy development
- 4) Engage in the strategic planning process to support the business
- 5) Reduce cost and corporate risk related to environmental issues and identify preferred alternative approaches

Environmental Policy reviews and analyzes proposed and final regulations, communicates potential issues to the Company, and is responsible for coordinating the overall strategy of the Company to ensure that the impacts are quantified, and possible future actions are integrated into the business plan. Current areas of focus include several proposed and final regulations that could impact AES's coal plants, including those owned or operated by DP&L. These regulations impact the disposal of coal ash, wastewater and air emissions, including greenhouse gases. Environmental Policy also closely monitors regulations which could potentially impact transmission and distribution operations.

The organizational chart for Environmental Policy is included as Environmental Policy – Exhibit 1.

Decision-Making and Control:

The day-to-day operational decisions are achieved by individuals within their given scope of authority and in accordance with DP&L policies and procedures. Federal and state regulatory initiatives with potential consequences to DP&L businesses are managed through Environmental Policy, with overall responsibility being that of the Vice President of Global Operations Support.

Internal and External Communications:

Promoting frequent, open communication on relevant environmental issues with our people, contractors and suppliers is an important responsibility within Customer Operations. Operating Managers are specifically accountable for clearly communicating environmental expectations for strong environmental performance to those people who report to them.

Environmental Policy supports the environmental communication efforts of Operating Managers by seeing to it that the business makes effective use of available communication means and

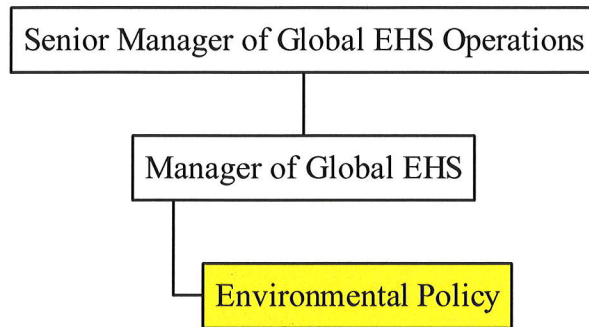
channels, such as annual environmental awareness training and DP&L's standard operating procedures.

It is the responsibility of Environmental Policy to manage the interface between Customer Operations and all relevant environmental regulatory agencies, including specific responsibilities for routine reporting, document submittals and correspondence as well as non-routine notifications and negotiations. Environmental Policy is accountable for assuring that all such communications with the environmental regulatory agencies are accurate and timely.

Responsibility for managing the process of environment-related communications with interested external stakeholders generally rests with Corporate Communications with input and guidance from Environmental Policy.

Environmental Policy – Exhibit 1

Organizational Chart for Environmental Policy



Functional Area:**Information Technology (Digital)****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**

Policy and Goal Setting:

DP&L's Digital 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 Digital group develops and enforces policies and general controls to minimize risks and support the governance mentioned above meet the needs of DP&L and its employees. Policies are developed by Digital 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 DP&L's regulating entities.

Digital policies and general controls are meant to provide direction on the use of Company sanctioned technologies and the associated data so that assets and information (Company and customer) are secured. Digital general controls ensure that proper policies, procedures and documentation exist and are followed. They are in place to verify the approval process, 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) Access control
- 4) Network and wireless security
- 5) Change Management
- 6) Operations Controls
- 7) Technology Disposal Controls

DP&L Digital policies can be found in Digital – Exhibit 2. Additional Digital related policies implemented at DP&L are documented and maintained by the AES Cyber Security Team.

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

Goal setting for Digital is a function of several drivers. The annual capital budgeting process identifies company initiatives that will require technology delivery and Digital support. The initiatives translate directly into goals for the Digital organization. In addition, periodic work and tasks are identified in the interest of maintaining the digital systems portfolio and ensuring

general availability. Lastly, Digital 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 Digital is aligned with similar activities within DP&L and AES. DP&L is awaiting a decision on a Stipulation and Recommendation (“Stipulation”), filed on October 23, 2020, that includes major systems associated with smartgrid and associated IT infrastructure that will be updated upon approval. Those systems are described in more detail in the Application and Stipulation filed in PUCO Case No. 18-1875-EL-GRD, incorporated herein by reference.

The Digital plan for Transitioning Utilities to the Energy Future guides the actions of the Digital organization. An AES Digital business plan exists to align with the overall business plan for the US SBU. The Digital Strategy addresses six major strategic themes Digital – Exhibit 3:

- 1) Customer Experience
- 2) Connected Enterprise
- 3) Digital Foundation
- 4) Smart Grid
- 5) Intelligent Enterprise
- 6) Digital Ecosystem

Digital maintains various technology roadmaps which assist in providing a big picture for major systems future. Development, integration and retirement of Digital systems are all considered as part of the roadmaps. The Digital Customer Initiative roadmap is included as Digital – Exhibit 4.

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

Organizational Structure and Responsibilities:

The Digital organization is part of the US SBU. It exists to serve AES Global interests and the US SBU companies and entities, which includes DP&L. It is led by the Global Chief Information Digital Officer and is comprised of technology areas and systems as follows:

US Digital Foundation – Responsible for the end-to-end development and maintenance of the core systems supporting DP&L’s utility operations.

- 1) Operations and Delivery
 - a) Data Center/Cloud Infrastructure – Responsible for Servers and Storage, Mainframe Computing, Data Center Facilities, Cloud Infrastructure

- b) Network/Telephony – Responsible for Internet Connectivity, Networking Infrastructure, and Telephony systems
 - c) Enterprise Applications – Responsible for SAP Financial, Supply Chain, Reporting, Payroll, HR, other business systems, application Integrations
 - d) T&D Applications – Responsible for Geographic Information, Outage Management, Metering, Work Management, Substation Maintenance, and Customer Support Systems (Call Center, Customer Billing)
 - e) Generation Applications – Responsible for Work and Asset Management, Asset Performance Management, Fuel Management, Lock Out Tag Out, and Generations associated Control Systems
 - f) Collaborations – Responsible for Workstation Computing, IT Service Desk, IT Field Services, IT Asset Management, Desktop Software Engineering, Mobile Devices, Operations Management, KPIs and Tracking
 - g) Architecture – Responsible for Cloud, Networking, and Active Directory Solution Designs
- 2) Mass Market – Responsible for External Mass Market Customer Experience and creating Mass Market Solutions, CRM, Customer Portal
 - 3) Workplace Experience – Responsible for internal employee experience through technology solutions, Office 365 Toolset
 - 4) Governance and Security – Responsible for IT General Controls, Digital Policies, DR and BC Planning, Auditing, Security Management, Budget and Budget Management, Project Management, Change Release Management, User Access Management

Digital Solutions and Innovation – Responsible for 3 core activities; Enterprise Architecture, Data Platforms, and Data Science to meet the needs of AES. The Enterprise Architecture function is designed to align the technology footprint of the AES US SBU with the business objectives and metrics, enable a more flexible technology delivery and lower TCO. The Data Platform and Data Science functions will focus on leveraging the data collected by AES systems and using analytics to drive business outcomes.

Digital Products and Ecosystem – Responsible for design, build and delivery of innovative digital products, services and solutions related to customer experience, engagement and energy management. Additionally, this organization will act as a change agent to drive customer and digital-centricity.

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 Digital organization is comprised of approximately 125 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 Digital systems portfolio for the entire US SBU. The Director of Digital reports to the AES Global Chief Digital Information Officer.

The Information Technology organizational chart is included as Digital – Exhibit 1.

Decision-Making and Control:

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

Performance against Digital commitments are tracked via KPIs and published on a routine basis as needed in a visual scorecard format. These KPIs cover key aspects of systems performance and projects that Digital does to support the company.

Internal and External Communications:

Internal communications involve communications between Digital and the business areas that subscribe to Digital services. Specific Digital 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:

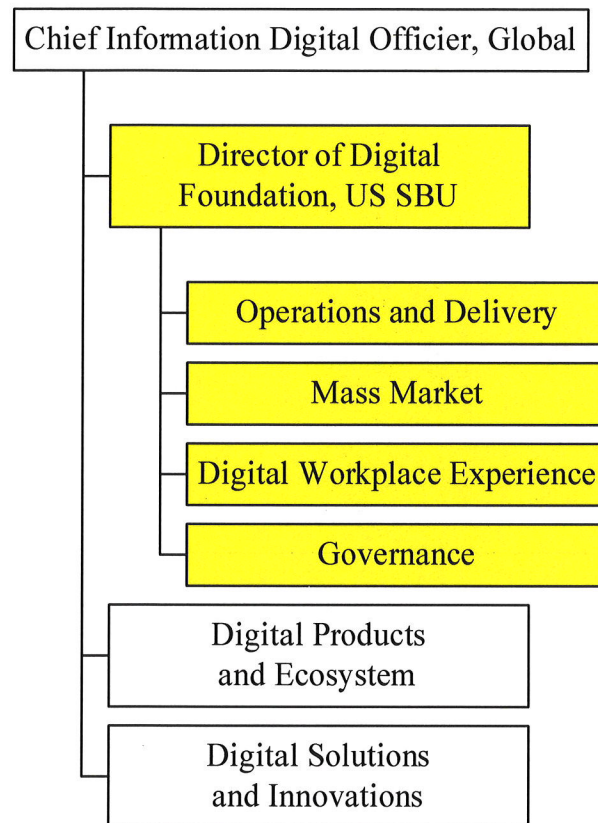
- 1) Face-to-face communication in meetings and individual conversations
- 2) Phone calls, conference calls and videoconferencing
- 3) Email
- 4) Instant messaging
- 5) Publication and dissemination of written materials

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.

Digital – Exhibit 1

Organizational chart for Digital



Digital Policies



AES US Strategic Business Unit ("US SBU")

Digital Operating Policies

AES US SBU DIGITAL POLICY

Policy Owner: US SBU Digital - Governance

Original Issue Date: May 2020

Revision Date: May 2020



US SBU DIGITAL POLICY

AES Confidential. For Internal use only

Contents

1.0	Introduction	1
1.1	Policy Statement	1
2.0	Scope and Applicability	1
2.1	Scope	1
2.2	Applicability	1
3.0	Definition(s)	2
4.0	Governance Controls	5
5.0	Access and Protection Controls	6
5.1	Systems and Applications Backup	6
5.2	Job and Batch Scheduling	6
5.3	Change Management	7
5.4	Access Management	7
6.0	New Digital Technologies	9
7.0	Related Policies and Standards	11
8.0	APPROVALS	12
9.0	Version Control History	13



Document Control No.: IT-000
Last Revised Date: 3-3-2020
Page 1

US SBU DIGITAL POLICY

AES Confidential. For Internal use only

1.0 Introduction

This policy ensures that development and maintenance of the Digital environment and development of Digital requirements are reliable, secure, and predictable.

The objective of this document is to describe controls, that when implemented by supporting standards and procedures, are designed to move any associated risks to an acceptable level.

1.1 Policy Statement

Information systems, and the information they contain, are fundamental to AES US SBU (Strategic Business Unit) daily operations and future success. AES US SBU will implement procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on our systems, and to ensure that the information is available to authorized persons when required based upon this policy document.

2.0 Scope and Applicability

2.1 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 designated. Please note that this Policy does supersede and replace any currently outstanding similar Policy at any of the aforementioned businesses and AES Corp.

2.2 Applicability

All users (Company employees, contractors, vendors or others) are responsible for adhering to this policy. This policy is applicable to all resources owned or operated by AES US Services LLC ("US Services"), each of its subsidiaries and any ventures that are controlled by US Services, where end-users and/or passwords are utilized;



Document Control No.: IT-000
Last Revised Date: 3-3-2020
Page 2

US SBU DIGITAL POLICY

AES Confidential. For Internal use only

3.0 Definition(s)

3.1 Backup Catalog

The catalog stores information regarding backups. The Catalog 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 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 any type of information stored on personal computers.

3.4 Scheduled Changes

Any change on frequency/scope to a standing server backup schedule.

3.5 Change Control

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

3.6 Change Management

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

3.7 Custodian

Individuals with the authority to approve changes to production environments

3.8 Batch and Job Scheduling

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



Document Control No.: **IT-000**
Last Revised Date: **3-3-2020**
Page **3**

US SBU DIGITAL POLICY

AES Confidential. For internal use only

3.9 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

3.10 End User

Individuals with authorized access to AES US 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

3.11 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

3.12 Privileged Access

Privileged access allows the management of logical access, change management, daily operations management and monitoring, as well as the ability to bypass technical security controls to read, write, modify, or communicate data/information that would not be accessible under an individual account. Privileged access includes access to other user's information granted by virtue of local or remote access in a support capacity.

3.13 Privileged Account Characteristics

(Accounts can have multiple characteristics)

3.13.1 Administrator

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

3.13.2 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

3.13.3 Shared

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



Document Control No.: **IT-000**
Last Revised Date: 3-3-2020
Page 4

US SBU DIGITAL POLICY

AES Confidential. For internal use only

3.13.4 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.

3.13.5 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.

3.13.6 Administrative Service

Any application, script or protocol that support the maintenance or administration of the technology assets (e.g. Servers, network devices, etc.).

3.14 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

3.15 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

3.16 IT Resource

Any service or component provided or maintained by IT.

3.1.17 Cloud computing

The term Cloud Computing refers to the delivery of on-demand computing services, such as processing, storage and communications, over the Internet (the "cloud") on a pay-for-use basis. Cloud computing includes not only the applications and services delivered over the Internet, but also the hardware and software needed to deliver those services. The three primary service models are:

- Software as a Service (SaaS): Examples include Google Docs, Salesforce, Workday, online collaboration solutions (e.g. Office365).
- Platform as a Service (PaaS): Examples include Google App Engine, Microsoft Windows Azure, Microsoft Live services, etc.
- Infrastructure as a Service (IaaS): Examples include Amazon Web Services (AWS), and VMware's VCloud, among others.



Document Control No.: IT-000
Last Revised Date: 3-3-2020
Page 5

US SBU DIGITAL POLICY

AES Confidential. For internal use only

4.0 Governance Controls

Governance control policy statements support the protection of AES Digital assets, and the alignment of AES Digital strategies and goals with the businesses objectives by identifying IT-related business risks, assessing risk severity, and determining appropriate risk responses for AES in accordance with its importance and potential impact to the organization

- 4.1 A process to assess Internal and external risks across AES US SBU is executed when a new Digital solution is being implemented, in order to identify and address key risks faced by AES US SBU. The risk analysis is based on the existing and approved ITGC (Information Technology General Control) catalog.
- 4.2 Internal self-assessments shall be performed on all information systems that house critical and financial AESUS SBU Application Information.
- 4.3 External providers for software and/or IT/Digital services must comply with the policy requirements included in this document. An independent report (SOC1/2) on controls at the Service Organization must be delivered to AES US SBU and reviewed by the Digital organization and the Business Application Owner.
- 4.4 Ensure business owners within the AES 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.
- 4.5 Measures must also be taken to evaluate if the new critical initiatives impact AES Global strategies and if so, ensure that the initiative is strategically aligned with AES strategy and that appropriate AES approvals are gathered.
- 4.6 All Company users must use company Digital resources only as authorized by and in accordance with this Policy. General principles on the appropriate use of all company Digital resources are outlined in Appendix A.
- 4.7 A process to assess or dispose decommissioned Digital assets shall be performed. Disposal principles on the adequate process of removing/decommissioning Digital assets are outlined in Appendix B.
- 4.8 All technology users will conduct themselves in accordance with the highest professional standards and in strict adherence with all laws (e.g. Sarbanes-Oxley Law), regulations (eg. NERC-FERC), policies (Digital, Accounting, etc.), and procedures. Misuse of privilege access, intentional wrongdoing or improper behavior that may compromise the company security and expose confidential/private information, may result in disciplinary action.
- 4.9 A process to manage and support installed resources including maintenance and tracking of inventory. The process should include guidance to establish adequate controls over lifecycle equipment and software.



Document Control No.: IT-000
Last Revised Date: 3-3-2020
Page 6

US SBU DIGITAL POLICY

AES Confidential. For internal use only

5.0 Access and Protection Controls

5.1 Systems and Applications Backup

5.1.1 Backups

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

5.1.2 Logging and Monitoring

All executed backups will be logged and monitored.

5.1.3 Catalog

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

5.1.4 Recovery Testing and Review

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

5.1.5 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.

5.2 Job and Batch Scheduling

5.2.1 Critical Jobs List

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

5.2.2 Job and Batch Scheduler access

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

5.2.3 Logging

All critical scheduled jobs and batch activities must be logged.

5.2.4 Monitoring/Failure Handling

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

5.2.5 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-000**

Last Revised Date: 3-3-2020

Page 7

US SBU DIGITAL POLICY

AES Confidential. For internal use only

5.3 Change Management

5.3.1 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.

5.3.2 Tracking System

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

5.3.3 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.

5.3.4 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.

5.3.5 Authorized Approval

Business and IT custodians will be identified and documented in an approval matrix. This approval matrix will be maintained on an annual basis at minimum or 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.

5.3.6 Segregation of Duties

Where applicable, enforce a segregation of duties between the individuals responsible for developing a change and migrating the changes into the production environment. Where applicable, programmers/developers should not have functional (business process) access in the production environment.

5.3.7 Review

The change control process and the custodian responsibilities are reviewed and monitored to ensure all process controls are operating effectively.

5.4 Access Management

5.4.1 Authentication

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

5.4.2 Account Provisioning

For AES US systems/applications, the Access Provisioning Processes requires appropriate management approval which must be documented and retained; additionally, all access permissions must be



Document Control No.: IT-000

Last Revised Date: 3-3-2020

Page 8

US SBU DIGITAL POLICY

AES Confidential. For internal use only

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.

5.4.3 Privileged Access

- Privileged access user accounts shall only be used when the additional privilege is required, and shall not be used for day-to-day activities
- All information revealed as a result of privileged access is protected and may not be given to any non-privileged user or to any other privileged user except as required to perform necessary work and approved by the relevant data owner.
- Individuals with privileged access must respect the privacy of system users, respect the integrity of systems and related physical resources, and comply with relevant laws, regulations and security requirements.
- Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.
- Individuals with privileged access must be aware of, and follow, change control processes before making changes to production systems.
- Privileged accounts are for administrative work only

5.4.4 Segregation of Duties

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

5.4.5 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.

5.4.6 Password Requirements

Password parameters should follow the AES Cybersecurity requirements (where there are no system constraints), regarding password complexity and timeframes removals.

Default Passwords in any system, application, device or database that resides in or connects to the AES network must be changed to complex passwords, either during the installation process or immediately thereafter before introducing into the production network.

All general user-level technologies require strong passwords, e.g. desktop/laptop, e-mail, devices, instant messaging, software services supporting business applications.

Admin-level technologies require extended length and complex passwords, e.g. root, enable, application administration accounts, shared accounts, system delivered/default accounts, service accounts, accounts and firefighter accounts.

5.4.7 Terminations

Disable or remove AES system user accounts for terminated AES personnel within ten (10) business days. Modify user access in AES systems for transferred AES personnel in accordance with their job responsibilities within ten (10) business days.

Document Control No.: **IT-000**Last Revised Date: **3-3-2020**Page **9**

US SBU DIGITAL POLICY

AES Confidential. For internal use only

5.4.8 Generic Accounts & Services

Where applicable lock, secure, or disable system-delivered and generic user IDs. At a minimum, remove default passwords and update passwords for these accounts annually.

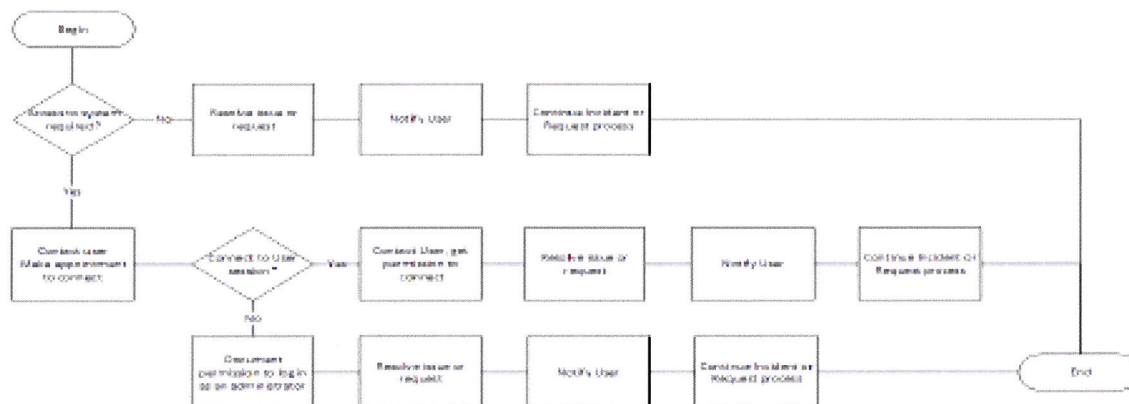
The use of the following administrative services is prohibited, unless there is a clear business need and an approved exception by Cybersecurity and Digital Management prior to the implementation of the device into the production network:

- File Transfer Protocol (FTP)
- Telnet
- Secure Shell Protocol (SSH)
- Simple Network Management Protocol (SNMP)

5.4.9 Access to Assets

Restrict Physical access to locations that house AES system assets such as (data centers and control rooms) to authorized personnel.

5.4.10 Support Access Flow



Support role implies access rights

Implies agreement from users to allow access to system and information/data at the start of a support incident or service request

Should be covered by professional conduct provisions (Code of Conduct) and meet the standards described by the access management policy

Users must be notified that they are granting permission

* Connecting to a user session means the support person is logged in as that user, with access to e-mail, and everything else as that user. User can see what is happening on the screen.

Logging in as administrator means the user cannot be logged on at the same time. Activity may not be shown on the screen

Either option can be done locally or remotely

6.0 New Digital Technologies



Document Control No.: IT-000
Last Revised Date: 3-3-2020
Page 10

US SBU DIGITAL POLICY

AES Confidential. For internal use only

6.1 Permitted Use – Cloud Services

Engagements for new systems must be evaluated for security and fitness for purpose before committing to use.

Any Company information deemed confidential or otherwise sensitive **must not** be stored, shared, or otherwise processed by a cloud computing provider unless the outsourced service enters into a legally binding agreement with AES US SBU to protect and manage the data with the minimum-security requirements described herein.

6.2 Evaluation Criteria

The AES US SBU has established guidelines for engaging with any cloud provider related to the types of information that may be stored in the cloud and the essential criteria for evaluation, particularly assessment of the potential security risk associated with storage of this data. Cloud providers are required to meet or exceed the AES US SBU controls.

6.3 Secure Channel Communications

A secure channel must exist for all data communications between any cloud service provider and AES US SBU users. Secure channels are required for both enterprise connections and end-point connections depending upon deployment and usage.

- Enterprise connections must be secured with a point-to-point method such as TLS, VPN, or SSL.
- End-point connections, such as laptops, PDAs, smartphones or other hand-held devices, must be secured with SSL, VPN, or similar tunnel-encrypting method.

6.4 Secure Access Controls

- Access controls for workforce members are governed by the AES US SBU Access and Protection controls, noted in Section 5 of this document
- Access controls for the provider are required to be at least as stringent as the controls established in the above-mentioned policy and must also include:
 - The principle of Least Privilege: Only those with a need to know shall have access to corporate data.
 - Monitoring: Access of corporate data must be recorded and reported.
 - Compartmentalization: Segregation of duties must be inherent in the provider's own access control procedures.
 - The use of shared logon credentials is prohibited.
- Strong Authentication – Where possible, administrative access to provider services should be protected with two-factor authentication mechanisms, such as security tokens, secondary passwords, or digital certificates.



Document Control No.: IT-000
Last Revised Date: 3-3-2020
Page 11

US SBU DIGITAL POLICY

AES Confidential. For internal use only

6.5 Secure Networking

The means and methods of safeguarding connectivity must be congruent with AES Cybersecurity requirements.

6.6 Backup Data

- Backup data must be available in the event of an emergency.
- Backup data should always be stored at a location separate from the primary cloud provider.

6.7 Audit Logging

- At a minimum, all providers must be able to make available reporting procedures on system utilization, performance statistics and access events.
- All suspicious activity should be investigated and documented.
- Logs should be archived and secured for a period consistent with Company policies and regulatory compliance.

6.8 Retention Policy

- Data stored at provider locations is still subject to the provisions defined in the AES Cybersecurity requirements.

7.0 Related Policies and Standards

- AES 2019 ITGC Catalog
- CyberSecurity Requirements



Document Control No.: **IT-000**
Last Revised Date: 3-3-2020
Page 12

US SBU DIGITAL POLICY
AES Confidential. For internal use only

8.0 APPROVALS

The following have reviewed and approved this business practice:

Approved:

<div>Antonio Narvaez</div> <div>Antonio Narvaez – US SBU Digital Director</div>	<div>5/15/2020</div> <div>Date</div>
---	--------------------------------------



Document Control No.: **IT-000**
Last Revised Date: 3-3-2020
Page 13

US SBU DIGITAL POLICY
AES Confidential. For internal use only

9.0 Version Control History

Date	Description of Changes	Author(s)	Approver(s)
May 8 th , 2020	Initial Policy creation	IT Governance Alejandro Ropero	Mike Birch



Document Control No.: IT-000

Last Revised Date: 3-3-2020

Page 14

US SBU DIGITAL POLICY

AES Confidential. For internal use only

Appendix A

Acceptable use principles:

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 resources including systems, services, and information 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, including members of management, co-workers, IT support and service desk staff.
- Do not permit anyone to share their accounts/passwords with you
- Do not attempt to access any company systems or accounts that you are not authorized to access (no hacking)
- 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 systems is the property of AES
- AES 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, voicemail, instant messaging, text messaging, or faxes, should never be considered private or secure

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

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.



Document Control No.: IT-000
Last Revised Date: 3-3-2020
Page 15

US SBU DIGITAL POLICY

AES Confidential. For internal use only

- 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
- 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

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

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

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

Document Control No.: **IT-000**

Last Revised Date: 3-3-2020

Page 16

US SBU DIGITAL POLICY

AES Confidential. For internal use only

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

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.

- Voicemail 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



Document Control No.: IT-000
Last Revised Date: 3-3-2020
Page 17

US SBU DIGITAL POLICY

AES Confidential. For Internal use only

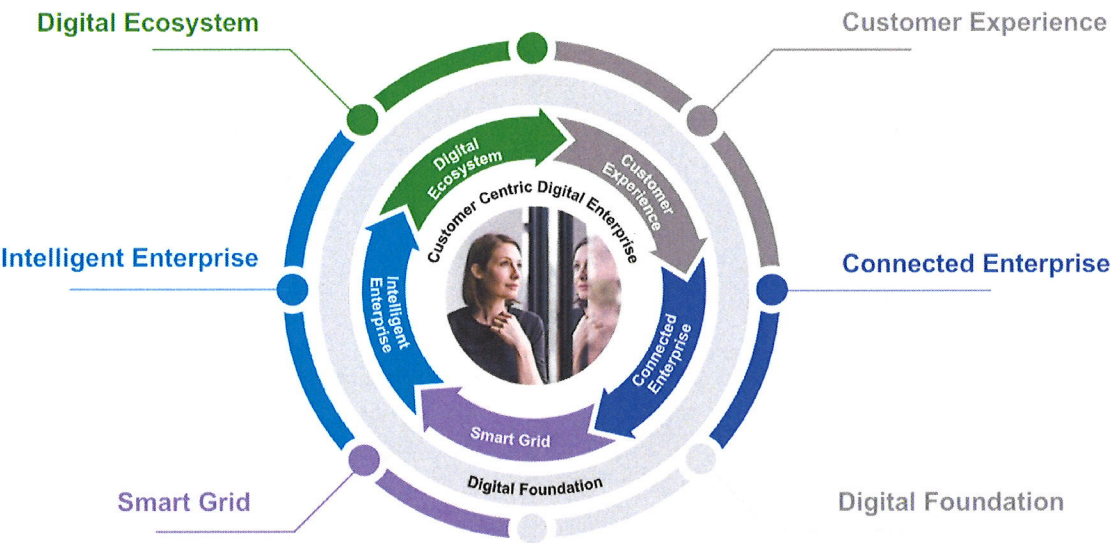
Appendix B

AES US SBU Technology Equipment Disposal principles:

- When Technology assets have reached the end of their useful life, they should be sent to the AES responsible facility for proper disposal.
- The AES responsible facility will securely erase all storage mediums in accordance with current industry practices and ensuring to meet legal data retention requirements.
- All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.
- Upon return, technology equipment cannot be sold to any individual.
- No computer equipment should be disposed of via dumps and landfill.
- All electronic drives must be demagnetized or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
- The AES responsible facility will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
- IT equipment with erased memory or storage technology will have the memory or storage device removed and it will be physically destroyed.
- The Digital Operations team might donate, recycle or properly dispose of outdated technology assets.
- Any equipment not in working order will be disposed, according to current environmental guidelines.
- The Digital Operations team has contracted with several organizations responsible for the properly equipment's disposal.
- Prior to leaving AES office premises, all equipment must be removed from the Information Technology inventory system.

AES Digital five-plus major strategic themes

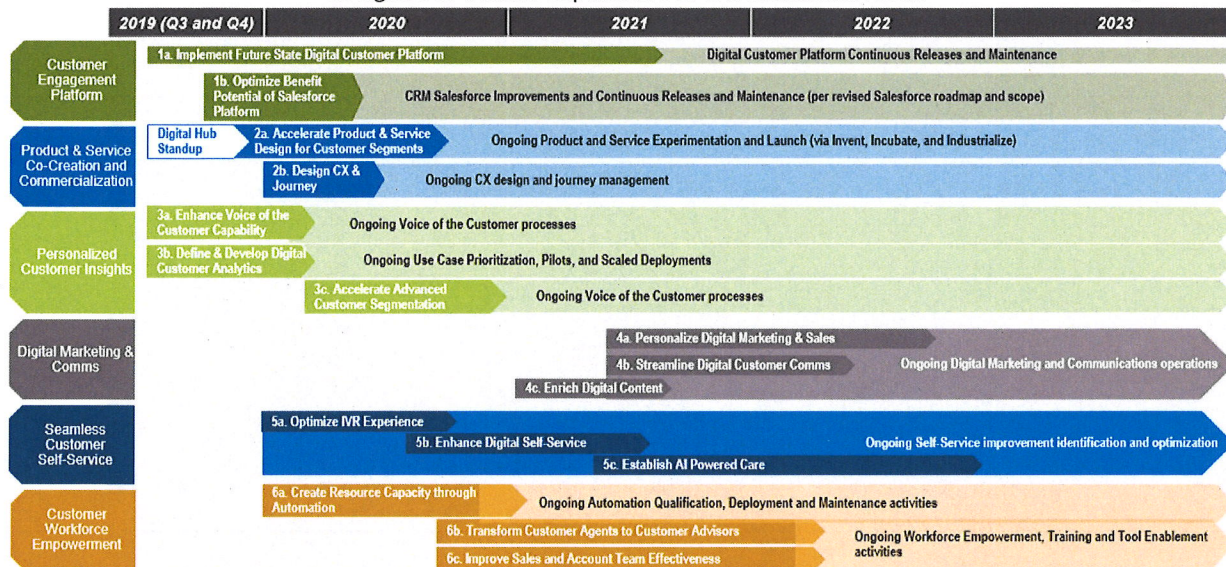
AES Digital Five Strategic Themes +



Digital – Exhibit 4

CUSTOMER INITIATIVE ROADMAP

The initiative roadmap is organized by capability and illustrates the sequence and timeline of defined initiatives designed to mature capabilities to a foundational level.



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 North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) compliance services for the transmission, distribution, 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 the 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 the Infrastructure Security managers report directly to the Chief Operating Officer (COO). This area maintains responsibility for the following utility activities:

Physical Security services are provided for 170+ locations within DP&L's geographical footprint and include substations, service centers, corporate offices, communication/microwave tower sites, remote storage yards and personnel security. Activities include:

- 1) Provide 24/7 security guard services for corporate offices and special assignments
- 2) Utilize 450+ electronic surveillance cameras at substations, service centers, tower sites and office facilities for situational awareness
- 3) 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
- 4) Manage all security operations from the security operations center in DP&L's service building
- 5) Supervise incident response, inquiries and investigations related to physical security and access control

Cyber-Security services are provided to Information Technology and Customer Operations by the AES Corporate Cyber Security team. Activities include:

- 1) Protect DP&L's computer network users, architecture and data from malicious activity using security methodologies, processes and technologies
- 2) Monitor DP&L's computer network, data center, workstations, electronic field terminals and personnel activity for external and internal threats
- 3) Provide awareness and training programs for DP&L personnel, contractors and vendors
- 4) Identify, classify and protect information assets throughout their lifecycles. DP&L's Information Classification Policy is attached as Infrastructure Security Services – Exhibit 2.
- 5) Supervise incident response, inquiries and investigations related to cyber-security and data protection

NERC CIP regulatory programs enforce mandatory requirements for in-scope business operations at transmission operation facilities that fall under NERC CIP v5 and NERC CIP 014 compliance standards. A complete listing of the security standards is included as Infrastructure Security Services – Exhibit 3. Activities include:

- 1) Address physical security risks and vulnerabilities related to the reliable operation of DP&L's bulk electric system, including transmission substations
- 2) Provide sabotage incident investigations and regulatory reporting
- 3) Identify and document the Bulk Electric System (BES) Cyber Assets associated with the critical Cyber Systems that support the reliable operation of DP&L's bulk electric system
- 4) Oversee security management controls to protect DP&L's high, medium, and low BES Cyber Assets according to DP&L's cyber security standards included as Infrastructure Security Services – Exhibit 4.
- 5) Manage DP&L's personnel with authorized cyber or unescorted physical access to DP&L's BES Cyber Assets, including contractors and service vendors, and ensure DP&L personnel have an appropriate level of personnel risk assessment, training, and security awareness
- 6) 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

- 7) Maintain a physical security program for the protection of DP&L's critical cyber assets
- 8) 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
- 9) Ensure the identification, classification, response, and reporting of cyber-security incidents related to DP&L's critical cyber assets
- 10) 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 the AES/DP&L Security Services is included as Infrastructure Security Services – 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 appropriately raised to a proper level of authority as required by DP&L's policies.

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.

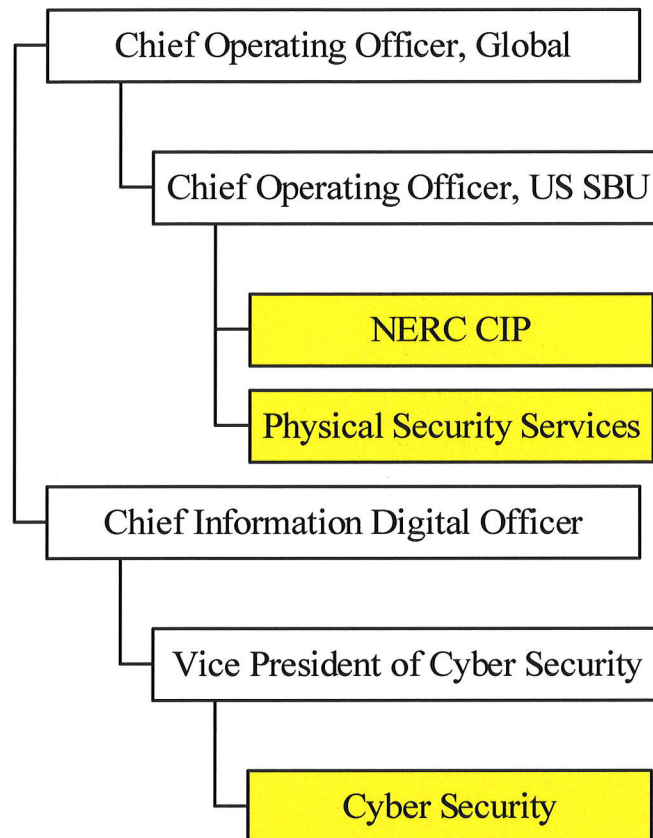
Internal and External Communications:

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.

Infrastructure Security Services – Exhibit 1

Organizational chart for DP&L's Security Services



Infrastructure Security Services – Exhibit 2



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 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. 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

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.

US SBU Information Classification Matrix				
Topic:	Public/Unclassified	Internal	Confidential	Restricted
Definition:	Information that is available to the general public and intended for distribution outside the organization. This information may be freely disseminated without potential Harm.	Information that is only intended for internal distribution among US SBU staff and authorized third parties (i.e. service providers, contractors and sub-contractors).	Confidential information is highly sensitive which is protected by legislation or regulations, legal contracts or internal policy.	Restricted information is highly sensitive which is protected by legislation or regulations, legal contracts or internal policy.
The examples listed are only provided for guidance purposes and should not be seen as an exhaustive list.	<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).
Possible consequences if information is mishandled	None	In the majority of instances the unauthorized disclosure would not significantly impact the organization.	The unauthorized or accidental disclosure of this information could seriously and/or adversely impact the US SBU, its staff, customers and business partners.	The unauthorized or accidental disclosure of this information could seriously and/or adversely impact the US SBU, its staff, customers and business partners.

US SBU Information Classification Matrix

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.


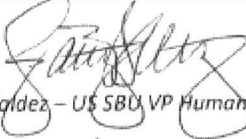
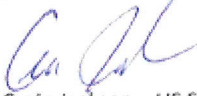

9.0 STANDARDS AND GUIDELINES

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

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

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	Sample text.	Sample text.	Sample text.	Sample text.

(Diagram 1)

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

Infrastructure Security Services – 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 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)

Infrastructure Security Services – Exhibit 4



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

AES United States

PO-003

Critical Infrastructure Protection (CIP) Cyber Security Policy

<u>APPLICABILITY</u>	<u>TYPE</u>	<u>SENSITIVITY</u>
Business Unit	Policy	Internal
<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	

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 1 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

Table of Contents

1.0	Applicability	3
2.0	Document Structure	3
3.0	Policy	3
3.1	General	3
3.2	AES US Culture of Compliance	3
3.3	Infrastructure Security Responsibilities	4
3.4	Governance	6
3.5	Monitoring	6
3.6	Specific Standards (High and Medium Impact BES Cyber Systems)	7
3.6.1	Personnel & Training (CIP-004)	7
3.6.2	Electronic Security Perimeter (CIP-005) including Interactive Remote Access	7
3.6.3	Physical Security of BES Cyber Systems (CIP-006)	8
3.6.4	System Security Management (CIP-007)	8
3.6.5	Incident Reporting and Response Planning (CIP-008)	10
3.6.6	Recovery Plans for BES Cyber Systems (CIP-009)	10
3.6.7	Configuration Change Management and Vulnerability Assessments (CIP-010)	11
3.6.8	Information Protection (CIP-011)	12
3.6.9	Declaring and Responding to CIP Exceptional Circumstances	12
4.0	Evidence Retention	13
5.0	Implementation Plan	13
6.0	Acknowledgements and Approvals	14
7.0	Revision History	14

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 2 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

1.0 Applicability

This policy applies to all employees, contractors, and vendors working at any of the AES United States (AES US) facilities and/or its subsidiaries who have physical, electronic, data or other access to Critical Infrastructure Protection (CIP) Bulk Electric System (BES) Cyber Systems classified with a high and medium impact rating. This policy also applies to Business Units (BUs), Infrastructure Security (IS), Distribution Operations (DO), Generation (Gen), Human Resources (HR), and Information Technology Services (ITS) who assist the NERC CIP Compliance Organization.

2.0 Document Structure

- 2.1 Cyber Security Policy - The policy document describes the overall CIP cyber and physical security for the AES US senior management.
- 2.2 Procedure Document (PR-###) - The procedure document is designed to provide the specific technologies, methodologies, responsibilities and applications used to meet the requirements of the individual standards. The procedure documents reference process documents which provide step-by-step instructions on how to perform the functions of the procedure.
- 2.3 Process Document (PROC-###) - The process document provides a detailed step-by-step instruction sequence on how specific functions are performed. The process document is used by the end user to complete the tasks that meet the NERC CIP compliance standards.
- 2.4 Evidence Documents (EV-###) - These forms/worksheets are used to collect and present the evidence of compliance for each individual requirement part.

3.0 Policy

3.1 General

- 3.1.1 Management is committed to securing its BES Cyber Systems in compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards CIP-002 through CIP-011. The purpose of this policy is to ensure affected parties are aware of this commitment and its applicability to high and medium impact assets identified through the PR-002 BES Cyber Systems Categorization process.
- 3.1.2 This AES US CIP Cyber Security Policy details requirements for identifying and protecting the BES Cyber Systems. The audience described in the applicability section of this policy shall comply with this CIP Cyber Security Policy, corporate policies, Information Protection and Security Standards and procedures, and Standard Conditions Contractor NERC/CIP Compliance Requirements.
- 3.1.3 This policy shall be reviewed by the AES US CIP Senior Manager at least once every 15 calendar months.

3.2 AES US Culture of Compliance

- 3.2.1 The Infrastructure Security Team (ISCT) within AES US endeavors to create a culture of compliance which goes beyond the mandated 15-calendar month training by

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 3 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

embedding compliance into the everyday workflow of individuals and sets the foundation and expectations for all personnel who work at AES facilities. The following methodologies are used to instill the culture of compliance throughout AES US:

- **Awareness** – The awareness program, detailed in PR-004 Personnel and Training, helps personnel to understand the compliance regulations and how it affects them in their day-to-day activities.
- **Communication** – The culture of compliance for AES US starts at the executive level. The executive leadership team provides clear communications concerning what is expected from each person regarding compliance requirements.
- **Education** – Ongoing training ensures personnel are fully up to speed on the latest requirements and their responsibilities.
- **Incident Reporting and Case Management** – The ISCT created clear processes for reporting any transgressions, or errors of compliance so that proper notifications can be made and the issue rectified. This process works both ways so any personnel who cause an issue can be notified and reminded of proper procedure.

3.2.2 Failure to fulfill compliance responsibilities is not acceptable as it negatively impacts the reliability of the Bulk Electric System. Individuals may be subject to disciplinary actions up to and including termination for failing to fulfill compliance responsibilities.

3.3 Infrastructure Security Responsibilities

3.3.1 **Infrastructure Security Compliance Team (ISCT):** The ISCT is responsible for developing and promoting a culture of integrity and compliance with laws and regulations for AES US and its subsidiaries. The responsibilities of ISCT, specific to the NERC CIP program include:

- Issuing a letter appointing CIP Senior Manager for the NERC CIP Compliance program. The CIP Senior Manager is identified by name, title, business phones, business address and date of designation. This letter is signed by a senior AES executive.
- Participating as a member of the NERC Governance and Executive Governance Committees.
- Reviewing relevant policies and monitoring performance.
- Document within 30 days of change of a CIP Senior Manager.

3.3.2 **NERC CIP Senior Manager:** A CIP Senior Manager designation letter created by ISCT and signed by a senior AES executive, to formally document the responsible AES US CIP Senior Manager. Responsibilities include:

- Acting as the senior officer of NERC CIP for AES US operations.
- Ensuring the AES US CIP Cyber Security Program complies with NERC CIP Reliability Standards CIP-002 through CIP-011.

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 4 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

- Assigning accountability to the appropriate level of management to ensure that the CIP Cyber Security Program receives the attention and support needed to comply with the NERC CIP requirements.
- Ensuring appropriate resources are available to develop, implement, and maintain the AES US CIP Cyber Security Program components.
- Delegating the authority of specific actions where allowed by CIP standards. See "PR-003 – R4 Delegation Authority" in secured documentation location.
- Reviewing and approving the AES US CIP Cyber Security Policy (this document).

3.3.3 CIP Compliance Team Members: Team Members include ISCT personnel and Business Unit Subject Matter Experts. Responsibilities include:

- Assisting Executive Management in ensuring team members are aware of the CIP Cyber Security Program and understand their role in complying with reliability standards.
- Meeting regularly with Executive Management to discuss CIP Cyber Security program matters.
- Recommending appropriate changes to the CIP compliance program.
- Providing periodic compliance reports, such as CIP Cyber Security program recommendations to Executive Management.
- Maintaining contact with FERC, NERC, and the Regional Entity (Reliability First [RF], who serves as the Compliance Enforcement Authority).
- Reporting CIP Compliance to FERC, NERC, and ReliabilityFirst.
- Leading internal and external assessments.
- Coordinating and tracking CIP compliance mitigation plans.
- Participating in internal CIP compliance meetings with impacted business units and in external industry compliance meetings as appropriate.
- Developing and implementing policies, procedures, work practices, and technologies that ensure CIP compliance with reliability standards and requirements.
- Reporting possible compliance issues or opportunities for improvement to the CIP Compliance Management.
- Developing relationships to gain insight on compliance best practices through participation in FERC, NERC and ReliabilityFirst conferences, events, forums, workshops, and gaining insight by cultivating relationships with neighboring utilities and trade associations.

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 5 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

3.4 Governance

- 3.4.1 **Governance Structure** – AES US has established a NERC CIP Oversight Committee which will help govern and monitor continuous compliance to NERC CIP standards and provide BES reliability. The membership of the NERC CIP Oversight Committee is listed in the EV-003 AES CIP Oversight Committee Members evidence document.

3.5 Monitoring

AES US implemented internal mechanisms for ensuring NERC CIP compliance. These internal mechanisms include, but are not limited to:

- 3.5.1 **Performance Metrics**: AES US has established performance metrics used to measure, evaluate, and improve the efficiency and effectiveness of the CIP Cyber Security Program. Performance metrics will provide the information necessary to make intelligent decisions to support NERC CIP compliance on an on-going basis. AES US has implemented enterprise-wide goals to support compliance to the NERC Reliability Standards.
- 3.5.2 **Mock Audits**: Designed to be like a NERC CIP Compliance Audit, mock audits are conducted by the Infrastructure Security Compliance Team and/or an external third-party consultant when an audit is not scheduled by the regional entity.
- 3.5.3 **Quality Assurance and Improvement Program (QAIP)**: An independent review of CIP compliance, including AES US and local facility processes and procedures, performed by QAIP board. A formal report on audit findings is issued to the NERC Compliance Director, AES US leadership and the Compliance Oversight committee.
- 3.5.4 **Internal Spot Checks**: Similar to a NERC or RF Spot Check but conducted by the ISCT and/or an external third-party consultant. As with a NERC or RF Spot Check, the internal spot check is focused on one Standard or a small group of similar Standards or it can be focused on specific requirement(s) of a Standard.
- 3.5.5 **Random Data Sampling**: Conducted by the ISCT and/or external third-party consultants as needed on large data populations. Random data sampling allows the ISCT to monitor compliance using random data sampling methodologies provided by NERC/RF.
- 3.5.6 **Reliability Standards Audit Worksheet (RSAW)**: The RSAW is a guide provided by the Electric Reliability Organization (ERO) that describes types of evidence Registered Entities may use to demonstrate compliance with a Reliability Standard. Consistent with NERC requirements, the ISCT will continue to effectively employ the use of RSAWs in audit preparation and completion.

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 6 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

3.6 Specific Standards (High and Medium Impact BES Cyber Systems)

AES US recognizes ensuring reliability of BES is a primary responsibility. AES US management achieves this by using defense in depth to protect BES Cyber Systems against compromise leading to misoperation or instability in the BES.

3.6.1 Personnel & Training (CIP-004)

- **Goals:** AES US management's goal is to provide an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems from compromise that could occur from individual's access.
- **Expectations:** The Personal Risk Assessment (PRA) will be performed at a minimum of every 7 years and the access granting process is configured so the PRA is performed prior to provisioning access to BES Cyber Assets or BES Cyber System Information (BCSI). Training appropriate to the role of the individual will be provided and reinforced using security awareness program.

A Transport Workers Identification Credential (TWIC) can be used as an alternative to the traditional background check process administered by Human Resources once the card has been verified through the Transportation Security Administration (TSA) Database.
- **Objectives:** HR will perform and maintain the personal risk assessment on individuals' or a valid TWIC card must be presented prior to granting access to BES Cyber Assets or BCSI. CIP Role Based Training will provide training to all those who has access or need access to the NERC assets or information. Training will be repeated for those needing unescorted physical and/or logical access to BES Cyber Assets at least once every 15-calendar months. The Security awareness program will be used to provide the security awareness using various methods such as quarterly newsletters, informational meetings, and posters. Infrastructure Security maintains a program to disable or modify physical/logical access for individuals who no longer need unescorted access and manage shared passwords known by those individual(s).
- **References:** Methodologies used and responsibilities assigned to meet the requirements of this standard are described fully in the PR-004 Personnel and Training procedure document and its associated process document(s).

3.6.2 Electronic Security Perimeter (CIP-005) including Interactive Remote Access

- **Goals:** AES US BES Cyber Systems will be protected by one or more Electronic Security Perimeters (ESP). AES US management's goal in establishing these perimeters is to prevent any unauthorized access to our critical systems. All applicable Cyber Assets are connected to a network via a routable protocol residing within a defined ESP, all the External Routable Connectivity is controlled via an identified Electronic Access Point (EAP),

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 7 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

and all the changes or modifications are monitored using change control and configuration management program.

- Expectations: ESP(s) will be protected, monitored for malicious activities, and access will be controlled. Access to the ESP will be granted only based on a defined business need and any remote access will be accomplished using an Intermediate System (Jump Box). All access events will be monitored, and incidents will be responded to using our Incident Response Program.
- Objectives: Appropriate programs, processes, and procedures will be established, maintained, monitored, evaluated, and tuned so they provide constant, reliable protection for the Electronic Security Perimeters and the BES Cyber Assets contained within. Any shortcoming or inconsistent performance in maintaining protections will be submitted for compliance evaluation.
- References: Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PR-005 Electronic Security Perimeters procedure document and its associated process document(s).

3.6.3 Physical Security of BES Cyber Systems (CIP-006)

- Goals: Establish physical security plan(s) to control and manage the physical access to the BES Cyber Systems.
- Expectations: Physical access controls will be deployed to allow unescorted physical access into each applicable Physical Security Perimeter (PSP) to only those individuals with authorized unescorted physical access. For High and Medium Impact BES Cyber Systems and their associated EACMS and PCA, two physical access controls, such as an access badge and a PIN number will be utilized. Unauthorized access will be monitored through the access points to the PSP.
- Objectives: Infrastructure Security will develop the physical security plan. The physical security plan details the approaches used to establish the Physical Security Perimeter (PSP) and will define both procedural and operations controls to restrict physical access to the BES Cyber Systems and Physical Access Control Systems (PACS).
- References: Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PR-006 Physical Protection of BES Cyber Systems procedure document and its associated process document(s).

3.6.4 System Security Management (CIP-007)

- Goals: Control and manage system security by specifying controls for ports and services, patch management, malicious code prevention, event monitoring, and system access control.

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 8 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

- **Expectations:** The configuration files will list the allowed ports for each BES Cyber Asset and their associated EACMS, PACS, and PCAs; all other ports will be denied, or a technical feasibility reference will be documented if appropriate. System owners will enable only logical network accessible ports deemed necessary for normal business or emergency operations and will document the reason for any open ports. The security patches per asset will be tracked, evaluated and deployed. Methods to deter, detect, or prevent malicious code will be deployed. Cyber Assets will be configured to log events, per Cyber System capability, and these events will be monitored to determine any security incidents. BES Cyber Systems will be configured to enforced to use of authentication for interactive user access where technically feasible.
- **Objectives:** The Infrastructure Security Compliance Team will develop, implement, and monitor controls to ensure that only the required ports and services are available, systems are patched on a consistent basis, malicious code prevention measures are in place, assets are configured to log events, and interactive user access is authenticated where technically feasible.
- **References:** Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PR-007 System Security Management procedure document and its associated process document(s).

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 9 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

3.6.5 Incident Reporting and Response Planning (CIP-008)

- **Goals:** Manage risk to the reliable operation of the BES as the result of Cyber Security Incident.
- **Expectations:** The processes to identify, classify, and respond to Cyber Security Incidents, both electronic and physical will be included in an Incident Response Plan (IRP). The 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 Incident Response Plan. Any changes to a Response Plan or lessons learned will be reflected in the Plan documentation within 90 days of the end of an exercise or actual event. Any individuals or groups with a defined role with the Incident Response Plan will be notified of the changes within the same 90-day period. Any changes to the roles and/or responsibilities within the Incident Response plan will be communicated to each individual or groups with a defined role in the Incident Response plan within 60-calendar days of the change being made.
- **Objectives:** The AES US Incident Response Plan will be used to respond to the security incidents relevant to CIP assets. The IRP will be applicable to all the High and Medium Impact BES Cyber Systems. E-ISAC will be informed, as required, within one hour of confirmation of security incident. For each reportable Cyber Security Incident, documentation of the incident and any forensic evidence obtained shall be kept for at least three years.
- **References:** Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PR-008 Incident Reporting and Response Planning procedure document and its associated process document(s).

3.6.6 Recovery Plans for BES Cyber Systems (CIP-009)

- **Goals:** Develop and implement the Recovery Plan and procedures to recover reliability functions performed by BES Cyber Systems.
- **Expectations:** A business continuity/disaster recovery plan shall be created, tested and maintained by asset type. The recovery plan shall describe the standardized approach the Infrastructure Security Compliance Team (ISCT) is taking on the backup and recovery of assets using "Backup and Recovery Procedures" per asset type. The backup and recovery procedures by asset type include the availability of spare components and the availability of the backups in case restoration of BES Cyber Assets is required.
- **Objectives:** The recovery plan, governed by the ISCT, shall include the minimum requirements for the backup and recovery procedures. The backup and recovery procedures shall include the procedures specific to the asset type. The recovery plan and all the associated procedures shall be tested at least once every 15-calendar months via tabletop methodology and through the testing of a representative sample of information used to

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 10 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

recover BES Cyber Assets to ensure the information is usable. Test of the recovery plan(s) through an operational exercise shall be performed at least once every 36-calendar months for High Impact BES Cyber Systems. Recovery from an actual incident can be considered as test of recovery plan. The recovery plan is updated based on the exercise or actual recovery within 90 days. Individuals and groups with a defined role within the recovery plan are notified of any changes and lessons learned within the same 90-calendar day period. Changes to the roles and/or responsibilities within the recovery plan are communicated to all relevant business units within 60 days of the change.

- References: Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PR-009 Recovery Plans for BES Cyber Systems procedure document and its associated process document(s).

3.6.7 Configuration Change Management and Vulnerability Assessments (CIP-010)

- Goals: Develop, maintain, and enforce configuration management and vulnerability assessment controls to prevent and detect unauthorized changes to BES Cyber Systems.
- Expectations: The ISCT shall maintain baseline configuration for applicable systems by individual cyber asset type. All changes to the Cyber Asset will follow the change control process.
- Objectives: The baseline configuration information at a minimum includes operating system or firmware, any commercially available or open-source application software intentionally installed, custom software installed, logical network accessible ports, and any security patches installed. Any changes to the baseline will be documented and authorized as part of the change management program. The baseline configuration shall be updated within 30-calendar days of an authorized baseline change. Impact on baseline, specifically those controls associated with CIP-005 and CIP-007, shall be evaluated prior to making changes in production assets. Where technically feasible, for baseline configuration changes to High Impact BES Cyber Systems a test environment shall be used prior to implementing the change in a production environment. To document the testing performed a list of cyber security controls tested will be created and will include the test results. A list of differences between the production and test environments with descriptions of how any differences were accounted for, with the test date will be maintained. Infrastructure Security shall conduct and document a paper or active vulnerability assessment at least once every 15-calendar months for all applicable systems. Where technically feasible, Infrastructure Security shall conduct an active vulnerability assessment at least once every 36-calendar months for High Impact BES Cyber Systems in production environment where the test is performed in a manner that minimizes adverse effect, or in the test environment that models the production baseline configuration.

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 11 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

- **References:** Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PR-010 Configuration Change Management and Vulnerability Assessments procedure document and its associated process document(s).

3.6.8 Information Protection (CIP-011)

- **Goals:** Develop, maintain, and enforce information protection controls to prevent and detect unauthorized access to BES Cyber System Information.
- **Expectations:** The Infrastructure Security Compliance Team will define the methods for identifying, designing, storing, protecting, transmitting, and destroying BES Cyber System Information (BCSI). Access to BCSI will be controlled based on need and is granted only after PRA and training completion. Infrastructure Security records the transfer, physical protect protection, sanitization and disposal of electronic storage media containing BCSI.
- **Objectives:** Infrastructure Security will deploy and maintain operational and procedural controls to identify, designate, store, protect, transmit, and destroy the BCSI. The Infrastructure Security Compliance team sanitizes electronic storage media prior to disposal and reuse outside of applicable systems. Discovery of unauthorized BCSI disclosure initiates an Infrastructure Security Compliance review and assessment with possible trigger of the Incident Response Plan.

3.6.9 Declaring and Responding to CIP Exceptional Circumstances

- **Goals:** Develop a process to invoke special procedures in the event of a CIP Exceptional Circumstance. This will allow for exceptions to normal policies, procedures and/or process that in the event of an emergency.
- **Expectations:** CIP Exceptional Circumstances are situations that involve or threaten to involve conditions that impact safety or BES reliability. Such circumstances might include, but are not limited to natural or manmade disasters, a risk of injury or death, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services that forces AES US personnel to respond and recover from it and may not have resources to collect evidence of compliance for certain requirements for the CIP standards.
- **Objectives:** As a CIP Exceptional Circumstance (CEC) can occur at any time, it is allowable for any AES US employee to declare a CEC and suspend evidence collection for a limited time as detailed in the applicable areas of the AES US Procedure and Process documentation. Once the CEC has been concluded, a summary of the event is written by the personnel involved and submitted to the Infrastructure Security team for review. The EV-003 CIP Exceptional Circumstance document is used to record the information pertaining to the potential CIP Exceptional Circumstance. The Infrastructure Security team

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 12 of 14



Original Issue Date: 09/01/2017

Last Revision: 01/09/2020

Revision Number: 5

coordinates with the CIP Senior Manager and any applicable delegates to determine if the event qualifies as a CEC and records the results of their investigation on the EV-003 CIP Exceptional Circumstance document. If necessary, a self-report will be created and submitted if the event was determined not meet the criteria for a valid CEC.

- References: Methodologies used, and responsibilities assigned to declare and evaluate CIP Exceptional Circumstances are located in the procedure documents where the use of CIP Exceptional Circumstances are permitted.

4.0 Evidence Retention

All business units shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period as part of an investigation.

- 4.1 Each business unit shall retain evidence of each requirement in the CIP standards for at least one full audit cycle.
- 4.2 In case of non-compliance, evidence shall be kept until mitigation is complete and approved or for the time specified above, whichever is longer.
- 4.3 Infrastructure Security shall keep the last audit records, and all requested and submitted subsequent audit records.

5.0 Implementation Plan

- 5.1 Accountably Policy Officers:
 - 5.1.1 Judi Sobecki – General Counsel and CIP Senior Manager
- 5.2 Effective Date: July 1, 2016 (Original Document)
 - 5.2.1 The revision of this document becomes current on the date the document is signed by the CIP Senior Manager.
- 5.3 Communication and Training Plan:
 - 5.3.1 AES US personnel are notified of the Cyber Security Policy as part of their initial and refresher CIP training.
 - 5.3.2 Presentations and Computer Based Training (CBT) will be performed as needed.
- 5.4 Sustainability Plan:
 - 5.4.1 This policy will be reviewed for accuracy and approved on at least once every 15-calendar months by the designated CIP Senior Manager.
 - 5.4.2 Upon change of CIP Senior Manager, the ISCT will initiate the change documentation required.

INTERNAL

Critical Infrastructure Protection Program (CIP) Cyber Security Policy

Page 13 of 14



Original Issue Date: 09/01/2017
 Last Revision: 01/09/2020
 Revision Number: 5

6.0 Acknowledgements and Approvals

The following have reviewed and approved this business practice:

Originated/Revised By:

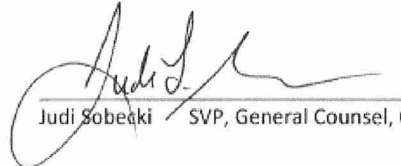
Date:


 Jeffrey K Fuller Director, Infrastructure Security

15 Jan 2020

Approved:

Date:


 Judi Sobecki SVP, General Counsel, CIP Senior Manager

1/15/2020

7.0 Revision History

Rev. #	Revised Date	Approved By	Revision Description
1	09/01/2017	Judi Sobecki	Original Document – US SBU Corporate version
2	02/12/2018	Judi Sobecki	References to "United States Strategic Business Unit (US SBU)" modified due to AES US reorganization.
3	07/30/2018	N/A	Appendix A updated to reflect changes to the Compliance Oversight Committee
4	01/14/2019	Judi Sobecki	Appendix A, The NERC CIP Oversight Committee Members list, was removed from this document and replaced by evidence document EV-003 AES CIP Oversight Committee Members. References to "annually" were replaced with "15-calendar months" where appropriate to better reflect the standards. Minor formatting and grammatical changes
5	01/09/2020	Judi Sobecki	Added verbiage to the Implementation plan, specifically section 5.2.1, to indicate when each revision of the Policy becomes the "current" or active revision of the document.

INTERNAL



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

AES United States

PO-003

Low Impact

Critical Infrastructure Protection (CIP) Cyber Security Policy

<u>APPLICABILITY</u>	<u>TYPE</u>	<u>SENSITIVITY</u>
Business Unit	Policy	Internal
<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	

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 1 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

Table of Contents

1.0	Applicability	3
2.0	Document Structure	3
2.1	Low Impact Cyber Security Policy	3
2.2	Plan Document (PL-area)	3
3.0	Policy	3
3.1	General	3
3.2	AES US Culture of Compliance	3
3.3	Infrastructure Security Responsibilities	4
3.4	Governance	5
3.6	Specific Standards (Low Impact BES Cyber Systems)	6
3.6.1	Cyber Security Awareness (CIP-003 Attachment 1 Section 1)	7
3.6.2	Physical Security Controls (CIP-003 Attachment 1 Section 2)	7
3.6.3	Electronic Access Controls (CIP-003 Attachment 1 Section 3)	8
3.6.4	Cyber Security Incident Response (CIP-003 Attachment 1 Section 4)	8
3.6.5	Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation (CIP-003 Attachment 1 Section 5)	9
3.6.6	Personnel Risk Assessments and Training	9
3.6.7	Declaring and Responding to CIP Exceptional Circumstances:	10
4.0	Evidence Retention	11
5.0	Implementation Plan	12
A.	Accountability Policy Officer(s):	12
B.	Effective Date: April 1, 2017	12
C.	Communication and Training Plan:	12
D.	Sustainability Plan:	12
6.0	Acknowledgements and Approvals	13
7.0	Revision History	13

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 2 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

1.0 Applicability

This policy applies to all employees, contractors, and vendors of the locations listed as containing Low Impact Systems in the EV-002 R1 BES Cyber System List having physical, electronic, data or other access to Critical Infrastructure Protection (CIP) Bulk Electric System (BES) Cyber Systems with a Low Impact classification. This policy also applies to Business Units (BUs), Infrastructure Security (IS), Distribution Operations (DO), Generation (Gen), Human Resources (HR), and Information Technology Services (ITS) who assist the NERC CIP Compliance Organization.

2.0 Document Structure

- 2.1 **Low Impact Cyber Security Policy** – This policy document describes the overall CIP cyber and physical security for AES US senior management.
- 2.2 **Plan Document (PL-area)** – The plan document is designed to provide the specific technologies, methodologies, and applications used to meet the standards. The plan documents may reference process or workflow documents providing more detailed instructions on how to perform the functions of the plan.

3.0 Policy

3.1 General

- 3.1.1 Management is committed to securing its BES Cyber Systems in compliance with the applicable North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards. The purpose of this policy is to ensure that affected parties are aware of this commitment and its applicability to Low Impact systems identified through the CIP-002 BES Cyber Systems Categorization process.
- 3.1.2 This Low Impact CIP Cyber Security Policy details requirements for identifying and protecting Low Impact BES Cyber Systems. The audience described in the applicability section of this policy shall comply with this Low Impact CIP Cyber Security Policy, corporate policies, and Information Protection and Security Standards and procedures.

3.2 AES US Culture of Compliance

- 3.2.1 AES US recognizes individuals and teams for demonstrating unique or extraordinary ways of promoting a culture of high ethics (including but not limited to reporting potential gaps in compliance) and reliability compliance.
- 3.2.2 The following methodologies are used to instill the culture of compliance throughout AES US:
 - Awareness – The awareness program, detailed in PL-003 Low Impact Cyber Security Awareness, helps personnel to understand the compliance regulations and how it affects them in their day-to-day activities.
 - Communication – The culture of compliance for AES US starts at the executive level. The executive leadership team provides clear communications

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 3 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

concerning what is expected from each person regarding compliance requirements.

- **Education** – Ongoing training ensures personnel are fully up to speed on the latest requirements and their responsibilities.
- **Incident Reporting and Case Management** – The ISCT created clear processes for reporting any transgressions, or errors of compliance so that proper notifications can be made, and the issue rectified. This process works both ways so any personnel who cause an issue can be notified and reminded of proper procedure.

3.2.3 Failure to fulfill compliance responsibilities is not acceptable as it negatively impacts the reliability of the Bulk Electric System. Individuals may be subject to disciplinary actions up to and including termination for failing to fulfill compliance responsibilities.

3.3 Infrastructure Security Responsibilities

3.3.1 **Infrastructure Security Compliance Team (ISCT):** The ISCT is responsible for developing and promoting a culture of integrity and compliance with laws and regulations for AES US facilities and its subsidiaries. The responsibilities of ISCT, specific to the NERC program include:

- Issuing a letter appointing CIP Senior Manager for NERC CIP Compliance program (identified by name, title, business phones, business address and date of designation).
- Participating as a member of the NERC Governance and Executive Governance Committees.
- Reviewing relevant policies and monitoring performance.
- Document within 30 days of change of a CIP Senior Manager.

3.3.2 **NERC CIP Senior Manager:** Introduction letter created by ISCT and signed by a member of the AES US executive leadership team, to formally document the responsible CIP Senior Manager. Responsibilities include:

- Acting as the senior officer of NERC CIP for AES US.
- Ensuring the each of the Low Impact CIP Cyber Security Plans comply with applicable NERC CIP Reliability Standards.
- Assigning accountability to the appropriate level of management to ensure that the Low Impact CIP Cyber Security Plans receives the attention and support needed to comply with the NERC CIP requirements.
- Ensuring appropriate resources are available to develop, implement, and maintain the AES US CIP Low Impact Cyber Security Plan components.
- Delegating the authority of specific actions where allowed by CIP standards.

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 4 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

- Reviewing and approving the Low Impact CIP Cyber Security Policy (this document).

3.3.3 **CIP Compliance Team Members:** Team Members include ISCT personnel and Business Unit Subject Matter Experts. Responsibilities include:

- Assisting Executive Management in ensuring team members are aware of the Low Impact CIP Cyber Security Plans and understand their role in complying with reliability standards.
- Meeting regularly with Executive Management to discuss CIP Cyber Security program matters.
- Recommending appropriate changes to the CIP compliance program.
- Providing periodic compliance reports, such as CIP Cyber Security program recommendations to Executive Management.
- Maintaining contact with FERC, NERC, and the Regional Entity.
- Reporting CIP Compliance to FERC, NERC, and the Regional Entity.
- Leading internal and external assessments.
- Coordinating and tracking CIP compliance mitigation plans.
- Participating in internal CIP compliance meetings with impacted business units and in external industry compliance meetings as appropriate.
- Developing and implementing policies, procedures, work practices, and technologies that ensure CIP compliance with reliability standards and requirements.
- Reporting possible compliance issues or opportunities for improvement to the CIP Compliance Management.
- Developing relationships to gain insight on compliance best practices through participation in FERC, NERC and Regional Entity conferences, events, forums, workshops, and gaining insight by cultivating relationships with neighboring utilities and trade associations.

3.4 **Governance**

- 3.4.1 **Governance Structure** – AES US has established a NERC CIP Oversight Committee which will help govern and monitor continuous compliance to NERC CIP standards and provide BES reliability. The membership of the NERC CIP Oversight Committee is listed in the EV-003 AES CIP Oversight Committee Members evidence document.

3.5 **Monitoring**

The ISCT implemented internal mechanisms for ensuring NERC CIP compliance. These internal mechanisms include, but are not limited to:

- 3.5.1 **Performance Metrics:** The ISCT has established performance metrics used to measure, evaluate, and improve the efficiency and effectiveness of the CIP Cyber Security Program. Performance metrics provide the information necessary to make intelligent

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 5 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

decisions to support NERC CIP compliance on an on-going basis. The AES US has implemented enterprise-wide goals to support compliance to the NERC Reliability Standards.

- 3.5.2 **Mock Audits:** designed to be like a NERC CIP Compliance Audit, mock audits are conducted by the Compliance Team and/or an external third-party consultant on an as-needed basis, for instance, a mock audit would be conducted after the implementation of a new CIP standard.
- 3.5.3 **Quality Assurance and Improvement Program (QAIP):** An independent review of CIP compliance, including AES US and local facility processes and procedures, performed by QAIP board. A formal report on audit findings is issued to the NERC Compliance Director, AES US leadership and the Compliance Oversight committee.
- 3.5.4 **Internal Spot Checks:** Similar to a NERC or Regional Entity Spot Checks but conducted by the ISCT and/or an external third-party consultant. As with a NERC or Regional Entity Spot Check, the internal spot check is focused on one Standard or a small group of similar Standards or it can be focused on specific requirement(s) of a Standard.
- 3.5.5 **Random Data Sampling:** Conducted by the ISCT and/or external third-party consultants as needed on large data populations. Random data sampling allows the ISCT to monitor compliance using random data sampling methodologies provided by NERC/RF.
- 3.5.6 **Reliability Standards Audit Worksheet (RSAW):** The RSAW is a guide provided by the Electric Reliability Organization (ERO) that describes types of evidence Registered Entities may use to demonstrate compliance with a Reliability Standard. Consistent with NERC requirements, the ISCT will continue to effectively employ the use of RSAWs in audit preparation and completion.

3.6 Specific Standards (Low Impact BES Cyber Systems)

AES US recognizes that ensuring reliability of the BES is a primary responsibility. The ISCT achieves this by using defense in depth to protect BES Cyber Systems against compromise that could lead to mis-operations or instability in the BES.

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 6 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

3.6.1 Cyber Security Awareness (CIP-003 Attachment 1 Section 1)

- **Goals:** The ISCT's goal is to provide an appropriate level of training, and security awareness in support of protecting BES Cyber Systems from compromise that could occur from external sources.
- **Expectations:** Through training, both initial and refresher training, quarterly newsletters, and cyber security awareness posters, AES US ensures its employees, vendors and contractors are made aware of security best practices used within the AES US footprint for the protection and stability of the BES.
- **Objectives:** To ensure employees, vendors and contractors who have physical or logical access to Low Impact BES Cyber Assets understand the reasoning and importance behind the security measures implemented within AES US facilities. The Cyber Security Awareness program also is used to instill the concept of "If you see something, say something" so all personnel take part in the security of AES US facilities.
- **References:** Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PL-003 Low Impact Cyber Security Awareness plan document.

3.6.2 Physical Security Controls (CIP-003 Attachment 1 Section 2)

- **Goals:** Establish physical security plan(s) to control and manage the physical access to Low Impact BES Cyber Systems.
- **Expectations:** Physical access controls, either manual or automated, shall be deployed to restrict unauthorized physical access to applicable Low Impact Cyber Assets or the areas where Low Impact BES Cyber Systems are located within AES facilities.
- **Objectives:** Develop a physical security plan detailing the approaches used to establish the Low Impact Physical Security Perimeter (LIPSP) and define both procedural and operations controls to restrict physical access to the BES Cyber Systems and Physical Access Control Systems (PACS).
- **References:** Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PL-003 Low Impact Physical Security Plan document.

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 7 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

3.6.3 Electronic Access Controls (CIP-003 Attachment 1 Section 3)

- **Goals:** BES Cyber Systems shall be protected by one or more cyber security controls to ensure only necessary inbound and outbound electronic communications are permitted between a Low Impact BES Cyber System(s) and a Cyber Asset(s) outside of the asset containing Low Impact BES Cyber Systems, use a routable protocol when entering or leaving the asset containing the Low Impact BES Cyber System(s), or are not used for time-sensitive protection or control functions between intelligent electronic devices. The cyber security controls shall be configured to allow only traffic with a specific business or emergency requirement and to deny all other traffic.

Where Dial-up communications are required, authentication shall be used, per Cyber System capability, to verify endpoints taking part in the communication process.

- **Expectations:** Security Perimeter(s) are protected, monitored for malicious activities, and limited to only necessary inbound and outbound directional routable protocol access. Access to the Security Perimeter is granted based on an identifiable business or emergency need. Appropriate events are monitored, and incidents are responded to using the Incident Response Program.
- **Objectives:** Appropriate programs, processes, and procedures are established, maintained, monitored, evaluated, and tuned so that they provide constant, reliable protection for the Low Impact Cyber Security Perimeters. Any shortcoming or inconsistent performance in maintaining protections must be submitted for compliance evaluation.
- **References:** Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PL-003 Low Impact Cyber Security Plan document.

3.6.4 Cyber Security Incident Response (CIP-003 Attachment 1 Section 4)

- **Goals:** Manage risk to the reliable operation of the BES as the result of Cyber Security Incident.
- **Expectations:** The processes to identify, classify, and respond to Cyber Security Incidents, both electronic and physical will be included in an Incident Response Plan (IRP). The 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 Incident Response Plan. Any changes to a Response Plan or lessons learned will be reflected in the Plan documentation within 90 days of the end of an exercise or actual event. Any individuals or groups with a defined role with the Incident Response Plan will be notified of the changes within the same 90-day period. Any changes to the roles and/or responsibilities within the Incident Response plan will be communicated to

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 8 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

each individual or groups with a defined role in the Incident Response plan within 60-calendar days of the change being made.

- **Objectives:** The AES US Incident Response Plan will be used to respond to the security incidents relevant to CIP assets. The IRP will be applicable to all the Low Impact BES Cyber Systems. E-ISAC will be informed, as required, within one hour of confirmation of security incident. For each reportable Cyber Security Incident, documentation of the incident and any forensic evidence obtained shall be kept for at least three years.
- **References:** Methodologies used, and responsibilities assigned to meet the requirements of this standard are described fully in the PL-003 Low Impact Cyber Security Incident Response plan document.

3.6.5 Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation (CIP-003 Attachment 1 Section 5)

- **Goals:** Manage the risk associated with the of the introduction of malicious code to Low Impact BES Cyber System(s) through the use of Transient Cyber Assets or Removable Media.
- **Expectations:** The processes used to mitigate the risk of the introduction of malicious code through the use of Transient Cyber Assets and Removable Media, both those maintained by AES and by third party contractors, will be included in a plan which details the methodologies used.
- **Objectives:** The AES US Transient Cyber Assets and Removable Media Plan will be used to detail the methodologies which can be used by each individual AES location which contains Low Impact BES Cyber System(s). The appendix of the plan document will detail the individual controls implemented at each specific AES location.
- **References:** Methodologies used are described fully in the PL-003 Low Impact Transient Cyber Assets and Removable Media Plan document.

3.6.6 Personnel Risk Assessments and Training

- **Goals:** Infrastructure Security shall provide an appropriate level of personnel risk assessment and training in support of protecting Low Impact BES Cyber Systems from compromise occurring from individual's physical and/or logical access.
- **Expectations:** CIP training and a Personal Risk Assessment (PRA) will completed for all personnel, employees and contractors, prior to approval and granting of unescorted physical or logical access to BES Cyber Systems. Identity verification and a seven-year criminal history check are included in the PRA. PRAs are updated at least every seven years after the initial PRA. A Transport Workers Identification Credential (TWIC) can be used as an alternative to the traditional background check process administered by

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 9 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

Human Resources once the card has been verified through the Transportation Security Administration (TSA) Database.

Training is given to individuals prior to being given physical and/or logical access to Low Impact BES Cyber Systems to build on the Low Impact Cyber Security Awareness program described earlier in this document. The training is repeated at least once every 15-calendar months to ensure personnel are aware of emerging cyber and physical security information.

- **Objectives:** AES US requires and maintains PRAs on individuals' prior to granting access to Low Impact BES Cyber Assets or information. ISCT creates and maintains a security training program, for both physical and cyber security, to ensure personnel understand security procedures prior to being given physical and/or logical access to Low Impact BES Cyber Systems. This security program will be repeated at least once every 15-calendar months to be used as a refresher and to ensure personnel are aware of emerging security issues. Infrastructure Security maintains a program to disable or modify physical/logical access for individuals who no longer need unescorted access and manage shared passwords known by those individual(s).

3.6.7 Declaring and Responding to CIP Exceptional Circumstances:

- **Goals:** Develop a process to invoke special procedures in the event of a CIP Exceptional Circumstance. This will allow for exceptions to normal policies, procedures and/or process that are necessary in the event of an emergency.
- **Expectations:** CIP Exceptional Circumstances are situations that involve or threaten to involve conditions that impact the safety of personnel or BES reliability. Such circumstances might include, but are not limited to natural or manmade disasters, a risk of injury or death, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services that forces AES US facilities to respond and recover from it and may not have resources to collect evidence of compliance for certain requirements for the CIP standards.
- **Objectives:** As a CIP Exceptional Circumstance (CEC) can occur at any time, it is allowable for any AES US employee to declare a CEC and suspend evidence collection for a limited time as detailed in the applicable areas of its Procedure and Process documentation. Once the CEC has been concluded, a summary of the event is written by the personnel involved and submitted to the Infrastructure Security team for review. The EV-003 CIP Exceptional Circumstance document is used to record the information pertaining to the potential CIP Exceptional Circumstance. The Infrastructure Security team coordinates with the CIP Senior Manager and any applicable delegates to determine if the event qualifies as a CEC and records the results of their investigation on the EV-003 CIP Exceptional Circumstance

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 10 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

document. If necessary, a self-report will be created and submitted if the event was determined not to meet the criteria for a valid CEC.

4.0 Evidence Retention

All business units shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

- Each business unit shall retain evidence of each requirement in the CIP standards for three calendar years.
- In case of non-compliance, evidence shall be kept until mitigation is complete and approved or for the time specified above, whichever is longer.
 - Infrastructure Security shall keep the last audit records, and all requested and submitted subsequent audit records.

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 11 of 13



Original Issue Date: 03/31/2017

Last Revision: 12/16/2019

Revision Number: 4

5.0 Implementation Plan

A. Accountably Policy Officer(s):

1. Judi Sobecki – CIP Senior Manager

B. Effective Date: April 1, 2017

C. Communication and Training Plan:

1. Presentations and Computer Based Training (CBT) will be performed as needed.

D. Sustainability Plan:

1. This policy will be reviewed for accuracy and approved once every 15-calendar months by the CIP Senior Manager.
2. Upon change of CIP Senior Manager, the ISCT will initiate the appropriate changes to the documentation required.

INTERNAL

Low Impact Critical Infrastructure Protection (CIP) Cyber Security Policy

Page 12 of 13



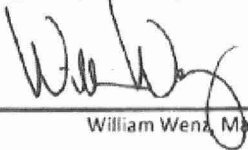
Original Issue Date: 03/31/2017
 Last Revision: 12/16/2019
 Revision Number: 4

6.0 Acknowledgements and Approvals

The following have reviewed and approved this business practice:

Originated/Revised By:

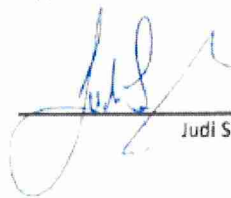
Date:


 William Wenz, Manager Infrastructure Security

12.16.2019

Approved By:

Date:


 Judi Sobecki – CIP Senior Manager

12/16/19

7.0 Revision History

Rev. #	Revised Date	Approved By	Revision Description
1	03/31/2017	Andy Horrocks	Original Document
2	02/14/2018	Judi Sobecki	Policy modified to reflect changes to the AES organizational structure.
3	01/14/2019	Judi Sobecki	Minor grammatical and content changes Removed Appendix A (list of Low Impact Systems/Facilities) and replaced it with a reference to the EV-002 R1 BES Cyber System list evidence document so the list of Low Impact BES Cyber Systems is consistent with all other CIP documentation. Appendix B – NERC CIP Oversight Committee Members was removed from this document and moved to a separate evidence document to allow the oversight committee to be consistent with the Cyber Security Policy for High and Medium impact systems.
4	12/31/2019	Judi Sobecki	Policy updated to meet the requirements of CIP-003-7: <ul style="list-style-type: none"> Removed references to LERC and LEAP. Included Attachment 1 Section 5 – Low Impact TCAs and Removable Media

INTERNAL

Functional Area:**Occupational Health and Safety Management****Policy and Goal Setting:**

DP&L's Safety policies comply 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 responsible to ensure that DP&L's policies meet or exceed the requirements set forth by all DP&L's regulating entities. The priority of all DP&L operating areas is to ensure the safety of all our employees, contractors and the public. DP&L takes this priority very seriously and incorporates safety into all aspects of operations. Safety takes precedence over all other utility operations and is listed first amongst the mission and values of the AES Corporation. DP&L's Occupational Health and Safety Management policies are included as Occupational Health and Safety Management – Exhibit 2.

AES and its subsidiaries strive to provide a place of employment for our employees and contractors that is free from recognized hazards and meets or exceeds governmental regulations regarding occupational health and safety. AES considers occupational health and safety a fundamental value of the organization and a key performance indicator of the overall success of the organization. AES expects that contractors working at AES owned, controlled, or managed facilities will share this value.

DP&L has developed and implemented an Occupational Health and Safety Management System, to meet all current applicable regulatory, AES Corporation and business occupational and safety requirements. A list of the requirements is included as Occupational Health and Safety Management – Exhibit 3.

Safety goals are set annually in support of DP&L and AES Corporate goals. Goals are divided into both leading and lagging indicators which are established to report safety performance and to encourage behaviors which improve safety performance. Goals for lagging indicators include meeting injury and illness rates and preventable vehicle accident rates. Goals for leading indicators include safety meeting attendance, safety inspections, and safety walks. The current safety goals are included as Occupational Health and Safety Management – Exhibit 4.

DP&L will establish and maintain programs for achieving its safety goals, objectives and targets. The written programs and procedures shall define the program requirements, implementation strategies, roles and responsibilities and training needs. The safety programs and procedures will meet or exceed the AES Environmental Health and Safety (EHS) standards.

Strategic and Long-Range Planning:

DP&L believes that all incidents are preventable. DP&L and AES maintain a thorough reporting system which requires that all incidents, near misses, workplace hazards and the use of stop work authority is documented, reported to AES and shared throughout DP&L and AES's operating companies. Through this sharing process AES helps all its operating companies learn and grow

from one another and DP&L benefits from safety lessons learned around the world. In addition, every DP&L employee is expected to attend a monthly safety meeting as well as DP&L's annual Safety Day. These events help to increase safety culture and awareness both at work and at home. DP&L management employees perform safety walks and jobsite reviews which encourage safe practices in the field and engages field employees with positive safety dialog. Through encouraging all employees and contractors to stay engaged in safety and being proactive on all safety topics, DP&L is aggressively pursuing an injury free workplace.

Organizational Structure and Responsibilities:

DP&L safety consists of 2 safety professionals and 2 elected union employees and is led by the Manager of the US Environmental, Health, and Safety for T&D Business. This organization is supported by the AES Corporate Safety and Health Department. Safety provides program development and implementation support for all employees. Safety ensures compliance with Occupational Health and Safety Management System, per all current applicable regulatory, AES Corporation and business occupational and safety requirements enhancing safety culture and the prevention of incidents and illnesses. Utility activities include:

- 1) Maintain compliance with all applicable EHS regulations, AES EHS Standards, and other requirements adopted by the business
- 2) Prepare annual work plans to achieve safety objectives and goals, with the approval of US SBU T&D EHS Manager
- 3) Maintain and continually improve the safety management system, control of documents and proactive safety programs at DP&L
- 4) Support compliance with the annual program of internal and external AES EHS audits at DP&L
- 5) Ensure hierarchy of controls in general hazard assessment and risk analysis, job hazard analysis and job safety analysis
- 6) Implementation and monitoring of the incident management program per OSHA and AES EHS standards. SIP Incident Investigation using TapRoot methodology
- 7) Develop and deliver EHS related orientation and training programs for DP&L employees
- 8) Visit job sites and facilities to conduct safety walks, work activity observations, safety inspections, and follow up
- 9) Maintain and continually improve the contractor management program compliance and special projects
- 10) Active participation in cross functional activities with IP&L EHS team
- 11) Encourage electrical safety programs in the general public with programs like "Think Hot, Stay Safe!" as well as information on DP&L's website
- 12) Track safety statistics for both leading and lagging indicators of safety performance. Monitor safety performance and trends to identify patterns which may justify a safety stand down

- 13) Develop safety materials for monthly safety meetings attended by all DP&L employees and contractors
- 14) Active participation in the DP&L's annual Safety Day event for all employees
- 15) Analyze conditions to proactively produce special safety alerts when warranted. For example, alerts may be generated if road construction produces a hazardous area which is safer to avoid and/or if hazardous weather is forecasted and employees need to exercise caution due to the conditions
- 16) Conduct contractor meetings to encourage open dialogue about safety, share best practices and to ensure that DP&L safety policies are known and followed by all those performing work on DP&L's property/system

The organizational chart for Occupational Health and Safety Management is included as Occupational Health and Safety Management – Exhibit 1.

Decision-Making and Control:

At DP&L safety decision-making and control goes beyond the Safety area. Safety decisions are made at all levels of the organization. Any DP&L employee no matter what position or skill, has the authority to stop any job at any time if they believe that the work being done isn't safe or if the job could be done in a safer manner. DP&L calls this our "Stop Work Authority". Using this authority is an obligation that every DP&L employee and contractor maintains if they see an unsafe situation.

Additionally, the safety responsibility is also shared by designated Safety Champions. Safety Champion is an annual role given to influential leaders throughout the business who share in the safety leadership for a period of time. These leaders reinvigorate Safety with new perspectives and ideas.

Performance against the Customer Operations goals is monitored and reported on a continuous basis, including monitoring of safety metrics, reliability targets, budgets and compliance. This monitoring helps to ensure that early warnings are in place when problems arise, allowing management to uncover trends in a timely manner to proactively address issues.

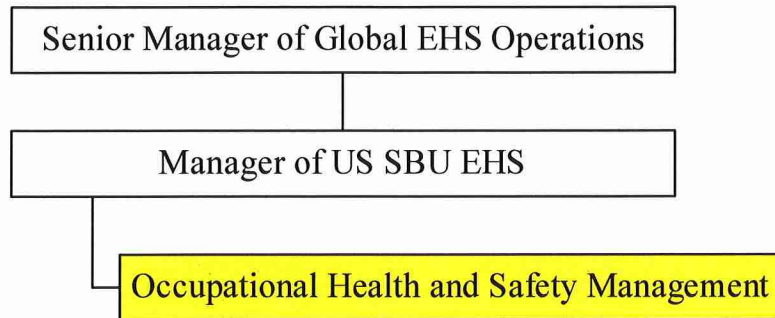
Internal and External Communications:

Internal and external communications are accomplished through a variety of channels including meetings, phone calls, conference calls, e-mails, public television, the Think Hot! Stay Safe! program, newspapers and the company website. Internal communications support the operations of all Customer Operations functional areas within DP&L. Safety works with Corporate Communications to develop messaging to communities and major accounts when inclement weather is forecasted, outages are planned and when any other safety concerns arise.

Communications with communities typically involve a variety of topics including electrical safety, generator safety during outages, pet safety, and holiday safety.

Occupational Health and Safety Management – Exhibit 1

Organizational Chart for Occupational Health and Safety Management



Occupational Health and Safety Management – Exhibit 2

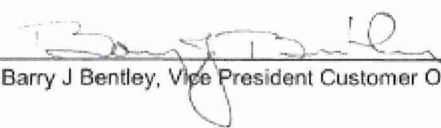
Safety and Health Policy

**Safety & Health Policy**
Dayton Power and Light

Dayton Power and Light puts safety first for our people, the contractors that work on our behalf, our customers and the individuals in the community in which we operate. We strive to conduct all of our work activities in a manner that promotes personal safety, health and well being. To ensure that we adhere to these standards consistently across our business, we have established this Safety and Health Policy with the following principles:

- **Dayton Power and Light leadership is ultimately responsible for safety performance.** While proper day-to-day safe work practices are everyone's responsibility, our leaders set occupational safety and health-related expectations, monitor safety performance against these measures, and hold themselves and our people accountable for meeting these targets.
- **Dayton Power and Light leadership will provide the appropriate resources, human and material, to ensure that all our people have the means to work safely.** Our leaders will ensure that the necessary engineering controls, people training and mentoring, procedures and equipment are provided to mitigate occupational safety and health risk.
- **Dayton Power and Light people will comply with all applicable occupational safety and health requirements.** Our people will identify, understand and comply with all occupational safety and health-related governmental regulations, and other applicable safety and health requirements including those imposed by DP&L policies, procedures and standards.
- **Dayton Power and Light contractors will to adhere to the same safety standards as our people.** We will ensure that contractors working for our business meet our occupational health and safety-related performance expectations and requirements or take appropriate steps if those expectations and requirements are not met.
- **Dayton Power and Light people will continuously strive to improve our Facilities occupational safety and health performance.** We will put into place and implement a safety management system (SMS) to set occupational safety and health goals, objectives and targets; commit to preventing injuries; measure safety and health performance; conduct regular safety and health audits or assessments to review compliance with applicable safety and health legal and company requirements; and make necessary SMS adjustments to achieve continuous improvement.

This Safety & Health Policy is based on our fundamental beliefs that everyone has a right to a safe workplace, all accidents can be prevented and working safely is a condition of employment. Adherence to these principles is mandatory for all our people.



Barry J Bentley, Vice President Customer Operations

9/16/2014

Date

Occupational Health and Safety Management – Exhibit 3

Regulatory and Other Safety Requirements

1) OSHA Standards

- a) OSHA 29CRR 1910 (<https://www.osha.gov/laws-regs>)

2) AES EHS Standards

- a) AES-STD-OHS01 - Safety Management System
- b) AES-STD-OHS02 - Hot work
- c) AES-STD-OHS06 - Confined Space
- d) AES-STD-OHS08 - Emergency Preparedness
- e) AES-STD-OHS10 - Enclosed Space Entry
- f) AES-STD-OHS14 - Electrical Safety
- g) AES-STD-OHS16 - Overhead Line Construction and Maintenance
- h) AES-STD-OHS17 - Underground Line Construction and Maintenance
- i) AES-STD-OHS18 - Substation Safety Standard
- j) AES-STD-OHS20 - Housekeeping
- k) AES-STD-OHS23 - Tree Trimming and Vegetation Management
- l) AES-STD-OHS25 - Machine Guarding
- m) AES-STD-OHS26 - Hearing Protection and Noise Reduction
- n) AES-STD-OHS27 - Illumination
- o) AES-STD-OHS29 - Defensive Driving - Vehicle Safety
- p) AES-STD-OHS30 - Heat and Cold Stress Prevention
- q) AES-STD-OHS03 - Contractor Safety Management
- r) AES-STD-OHS04 - Fall Protection
- s) AES-STD-OHS05 - Work Zone Traffic Control
- t) AES-STD-OHS07 - Control Hazardous Energy Sources - LOTO (T&D)
- u) AES-STD-OHS11 - Electrical Safety Qualification for T&D
- v) AES-STD-OHS12 - Incident Management
- w) AES-STD-OHS13 - Job Safety Analysis and Pre-Job Briefing
- x) AES-STD-OHS15 - Live Work
- y) AES-STD-OHS19 - Personal Protective Grounding
- z) AES-STD-OHS24 - Hoisting and Rigging
- aa) AES-STD-OHS31 - AES Proactive Safety Standard
- bb) AES-STD-OHS33 - Unmanned Aerial Vehicles (UAV) Safety
- cc) AES-STD-OHS34 - Excavation Safety
- dd) AES-STD-EHS02 - AES External EHS Audit Program
- ee) AES-STD-ENV02 - Spill Prevention and Containment
- ff) AES-STD-ENV03 - Hazardous and Special Waste Requirements

- gg) AES-STD-ENV04 - Chemical and Raw Material Management
- hh) AES-STD-ENV05 - PCB Management
- ii) AES Internal EHS Audit Standard

2.1) Programs and procedures associated (Listing of all DP&L Safety Policies)

- a) Bloodborne Pathogens
- b) Cell Phone and Two-Way Radio Use While Driving
- c) Confined Space
- d) Contractor Safety Management
- e) Defensive Driving
- f) Electrical Safety Qualification
- g) Emergency Action Plans
- h) Enclosed Space Entry
- i) Excavation of Underground Conductors
- j) Facility Lockout Tagout
- k) Fall Prevention
- l) Flame Resistant Clothing
- m) Grounding
- n) Hazardous Communication
- o) Hearing Protection and Noise Reduction
- p) Heat and Cold Stress Prevention
- q) Hoisting and Rigging
- r) Housekeeping
- s) Illumination
- t) Incident Management
- u) Lead Awareness and Protection
- v) Live Line Work
- w) Machine Guarding
- x) Occupational Dog Bite Safety
- y) Open Flame and Welding Permitting Requirements
- z) Overhead Line Construction and Maintenance
- aa) Personal Protective Grounding
- bb) Pre-Job Briefing and Job Safety Analysis (JSA)
- cc) Proactive Safety
- dd) Safety and Health Policy
- ee) Safety Facility Inspection and Hazard Identification Guidelines
- ff) Safety Management System
- gg) Safe Parking and Parking Lot Use
- hh) Substation Entry
- ii) Substation Personal Protective Grounding
- jj) Transmission and Distribution Lockout Tagout (Band and Tag)

- kk) Underground Line Construction and Maintenance
- ll) Vegetation Management
- mm) Work Zone Traffic Control

3) Documents

- a) DP&L Safety Manual
- b) AES US SBU Transmission and Distribution EHS Terms and Conditions
- c) AES US SBU Contractor Management Guide

4) Other requirements adopted by the organization

- a) U.S. Department of Transportation (<https://www.transportation.gov/>)

Occupational Health and Safety Management – Exhibit 4

DP&L Safety Goals, Objectives and Targets

GOAL	Weightage	Target	Achievement	
Fatality (AES People + Contractors)	50%	Zero	Target Lower Limit	100% 0%
Non-Injury SIP Rate (AES People + Contractors)	25%	1.2	Upper Target Lower Limit	200% of target 1.2 < Target
Safety Meetings (AES People + Contractors)	12.5%	95%	Upper Target Lower Limit	200% of target 100% of target < Target
Safety Walks	12.5%	99	Upper Target Lower Limit	200% of target 100% of target < Target

Functional Area:
Supply Chain

SFR Reference

(B)(9)(b)(v) Materials and inventory management and control
Staff Letter

Policy and Goal Setting:

Supply Chain policies are developed by Global Supply Chain management under the guidance of AES's management and AES's board of directors. All parties are equally responsible to ensure that the policies meet or exceed the requirements set forth by all DP&L's regulating entities. Supply Chain personnel are also expected to conduct business in accordance with the AES Code of Conduct and AES Values.

The first priority of all DP&L areas is to ensure the safety of all employees, contractors and the public. Supply Chain prioritizes safety and incorporates it into all aspects of operations. An example of incorporating Safety into all activities in Supply Chain includes using Avetta software which prequalifies potential contractors on a variety of safety topics. Additionally, all employees are required to attend monthly safety meetings.

Annual Supply Chain goals and objectives are set in support of company and corporate goals. Goals include targets for safety, savings, inventory and sourcing Key Performance Indicators (KPIs) and training. A listing of applicable supply chain KPIs are included as Supply Chain – Exhibit 2.

Strategic and Long-Range Planning:

Supply Chain updates its strategic plan annually for budgeting purposes and long-range planning with regard to inventory levels, personnel, equipment and service needs. Forecast and actual information is obtained from all business areas.

Supply Chain has the following short- and long-term goals that support the AES Corporate business plan:

- 1) Meet monthly safety meeting attendance and safety walk requirements
- 2) Increase focus on efficiencies from the Global Category Program Governance and Structure to deliver savings through sourcing activities that directly contribute to the target financial goals
- 3) Implement Supply Chain Digitalization solutions to increase efficiency on the Procure to Pay process and to improve internal customer purchasing experience
- 4) Create a clear demand planning strategy to allow the identification of opportunities for predictive analytics and pattern recognition to improve total inventory management and forecasting

- 5) Implement a supplier relationship management tool to regularly evaluate performance and promote development of critical suppliers in alignment with asset management strategy

Organizational Structure and Responsibilities:

Global Supply Chain consists of approximately 170 employees led by the Global Supply Chain Managing Director, and a Supply Chain Shared services Center of approximately 50 employees. There are five main divisions that are responsible for the following activities:

Category Management is responsible for the sourcing and contracting of goods and services related to all areas of AES's businesses, including DP&L. Activities include:

- 1) Develop and maintain relationships with internal customers and suppliers in order to procure the best quality and price of goods/services when they are needed
- 2) Evaluate performance and promote development of critical suppliers
- 3) Negotiate contracts, including terms and conditions
- 4) Maintain pipeline of upcoming projects
- 5) Continuously strive to include multiple and diverse suppliers in bid events

Logistics and Demand Planning is responsible for maintaining, distributing, replenishing and securing inventory. Activities include:

- 1) Issue inventory according to requests made by internal customers
- 2) Cycle counts to ensure the accuracy of physical inventory
- 3) Plan and replenish stock to maintain an optimum level of inventory for ongoing and emergency operations

E-Sourcing and Digitalization is responsible for technological integration, modernization and digitalization of Supply Chain activities. Activities include:

- 1) Implementation of new buying channels to improve internal customer and supplier procurement experience
- 2) Development of opportunities for automation, artificial intelligence solutions

Supply Chain Shared Services Center is responsible for providing procurement support among other activities such as:

- 1) Vendor and materials data management
- 2) Purchase order follow up and maintenance
- 3) Purchase order creation

Governance Standards and Systems is responsible for managing, controlling and developing the guidelines for functional system configuration, Policies and KPIs structures to control the global activity and performance of Supply Chain and its Shared Service Center.

The organizational chart for Supply Chain is included as Supply Chain – Exhibit 1.

Decision-Making and Control:

Supply Chain 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 policies and procedures. Policies and procedures guide decisions made during the course of business and set up approval hierarchies with regards to purchase requisitions, purchase orders, contracts and inventory levels and adjustments. A listing of applicable supply chain policies is included as Supply Chain – Exhibit 3.

Performance against Supply Chain goals is monitored and reported on a continuous basis, which includes monitoring of safety, diversity and overall spend and inventory metrics. 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:

Supply Chain holds staff meetings between leadership and direct reports on a monthly and intermittent basis. Reporting on Supply Chain metrics is published in a central online location for all team members to access. Oftentimes, reports and other communications are circulated via email and conference calls as well. Internal communications also correspond to supporting the operations of other functional areas of DP&L. These communications frequently happen through Ariba, SAP or other applications and include purchase requisitions, inventory requisitions and contract compliance and approval.

External communications with DP&L's suppliers occur as needed through a variety of means. Bids are obtained through written communications or by use of an e-sourcing tool, Ariba. Other communication venues used with suppliers include emails, phone calls and face-to-face meetings.

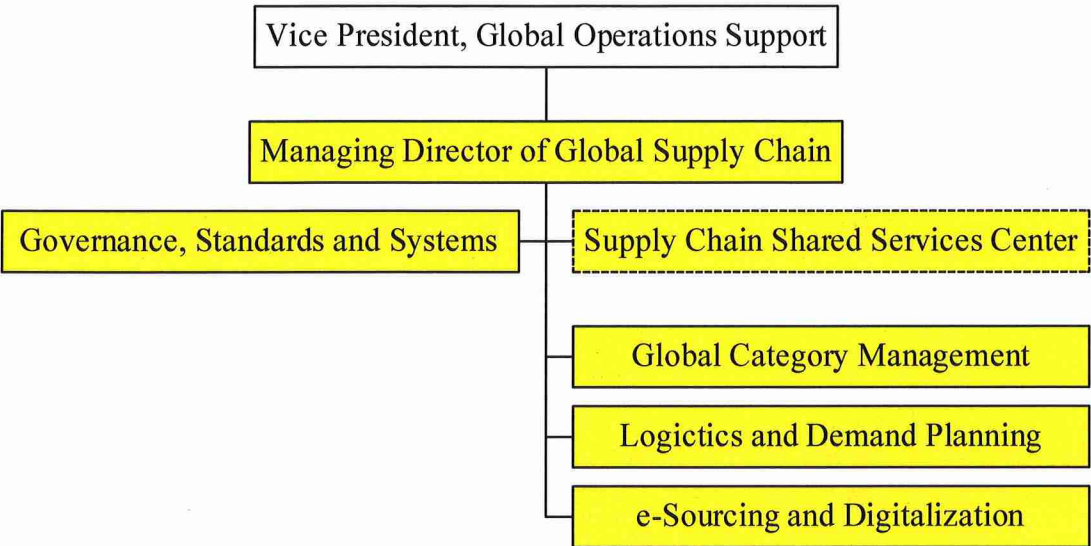
Staff Letter - DP&L's processes and controls associated with its internal controls over the issuance and return of materials and supplies associated with storm restoration equipment, specifically storm skid kits and the return of unused supplies:

DP&L provides storm kits (aka storm skids) to visiting mutual aid crews as an efficient way to distribute commonly used materials and equipment during a storm event. Each kit provides a variety of materials which field personnel have determined will likely be needed for the current storm. Typically, the kit will include ground wire, tri-plex service wire, insulators, fuses, connectors, tags and other appropriate restoration materials. Storeroom personnel record the materials provided to crews and the receiver (field crew) signs for the material. Throughout the storm event crews will continue to request additional materials as required for their assigned

jobs. As those materials are issued to crews, they are tracked and logged by storeroom personnel. Upon completion of the storm, crews will return any unused materials to the storeroom, and storeroom personnel will complete a material charge recovery form which is signed by the crew returning the materials. Finally, storeroom personnel enter all the information into DP&L's material tracking and inventory system and begin a review process to ensure that all materials have been charged to the appropriate accounts. Additional detail on this process can be found on Supply Chain – Exhibit 4.

Supply Chain – Exhibit 1

Organizational chart for Supply Chain



Supply Chain – Exhibit 2

Listing of Supply Chain Key Performance Indicators

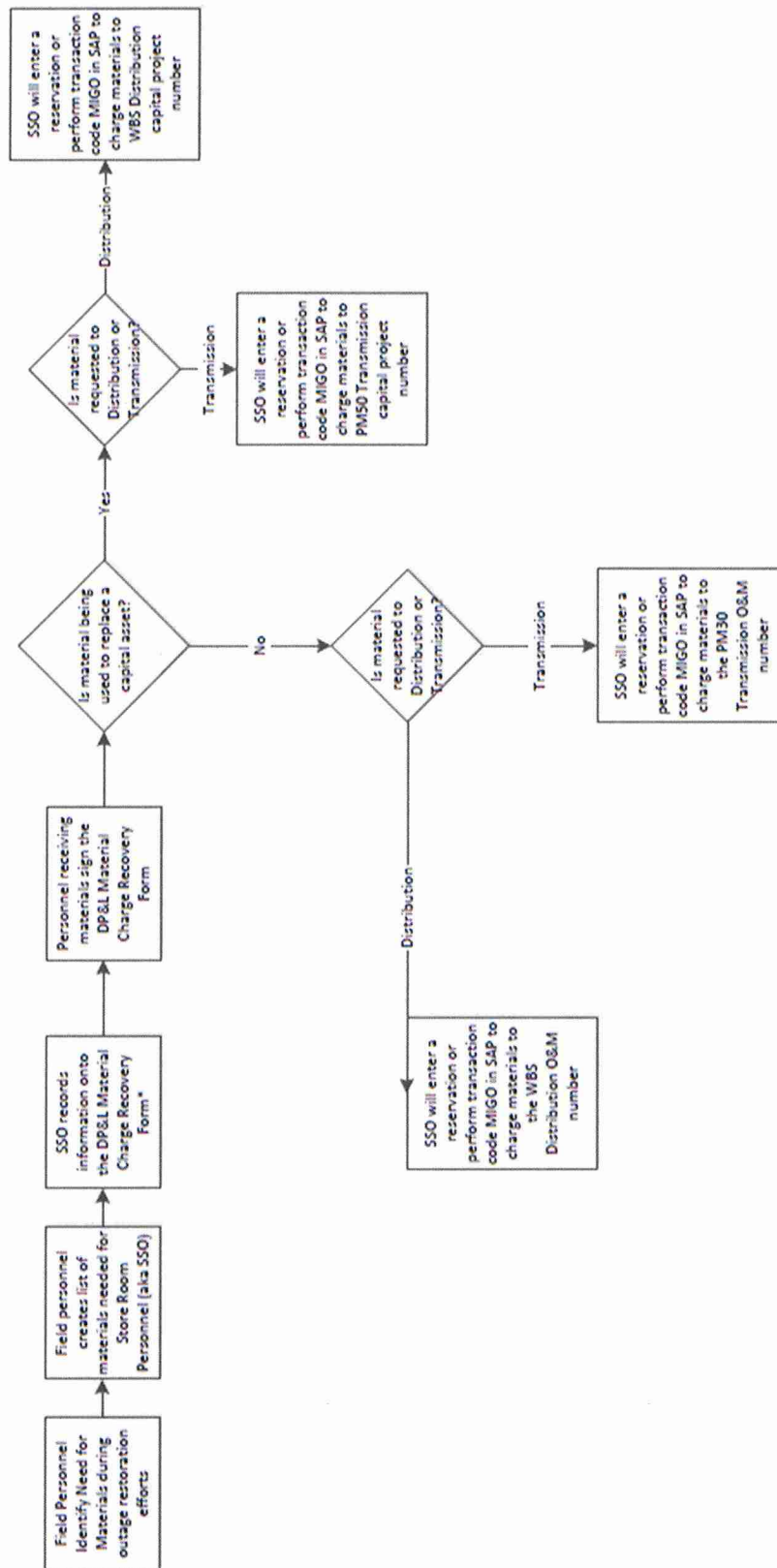
- Savings against budget
- Purchase Requisition to Purchase Order Cycle Time
- Purchase Requisition Days Outstanding
- On Time in Full Supplier to Warehouse
- Inventory KPIs:
 - Inventory Levels
 - Days in Advance for Reservations
 - Aging Reservations
 - On Time in Full Warehouse to Customer
 - Warehouse Returns

Supply Chain – Exhibit 3

Listing of Supply Chain Policies

- AES Global Procure to Pay Policy
- AES Global Non-Fuel Inventory Policy
- US SBU Expenditure Approval Policy
- AES Code of Conduct

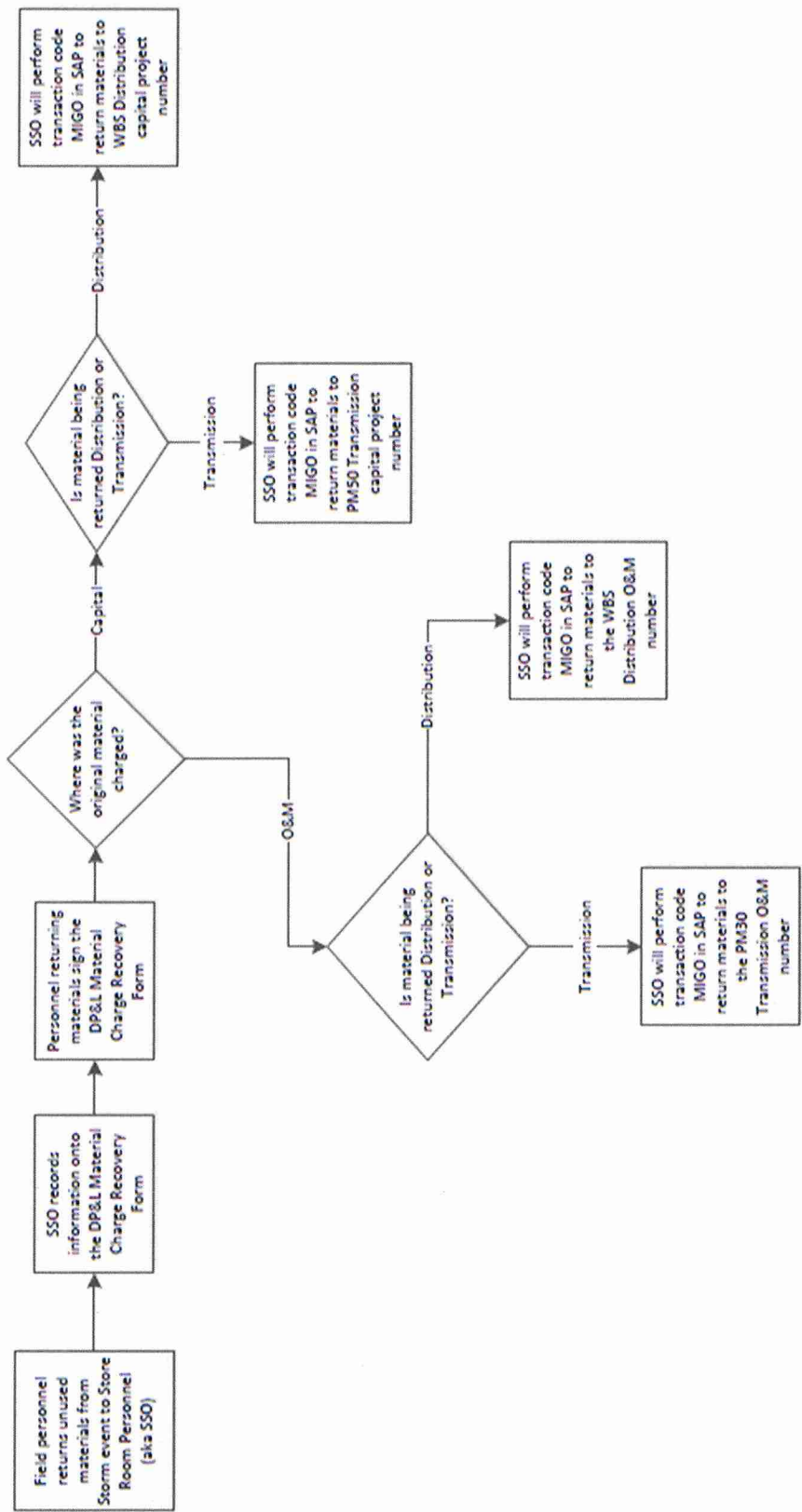
Supply Chain – Exhibit 4

Process for Storm Material Charges

* Store Room personnel record the materials removed from the store room or material yard (i.e. where poles and reels of cable are kept) on a DP&L Material Charge Recovery Form. Each store room location will have their own set of records/sheets.

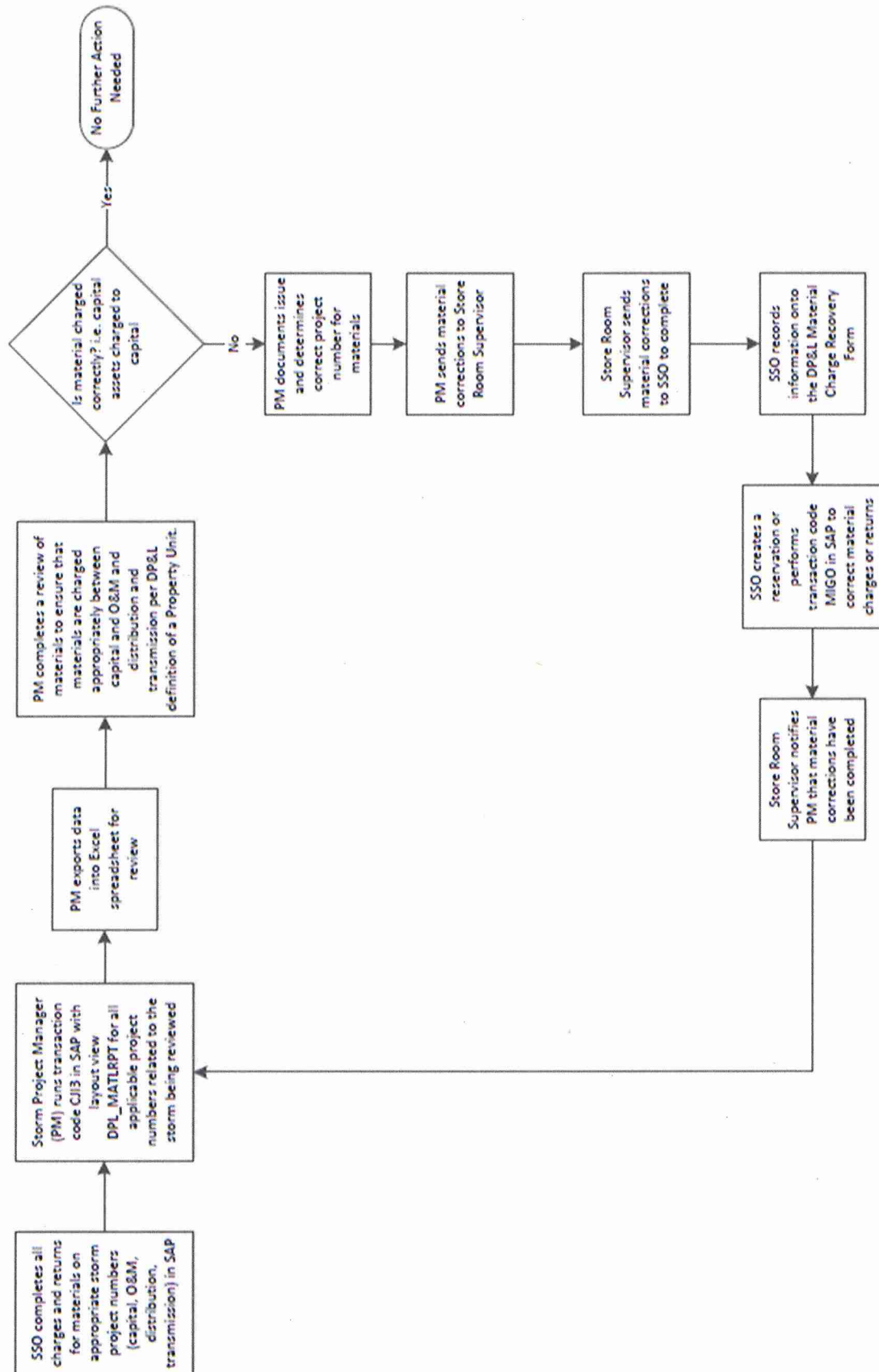
Mutual Aid crews are typically provided with storm skids containing various materials used during outage restoration upon arrival on DP&L property. If additional materials are needed by Mutual Aid crews, they will always be accompanied by a DP&L employee to assist with the storm materials process.

Process for Storm Material Returns



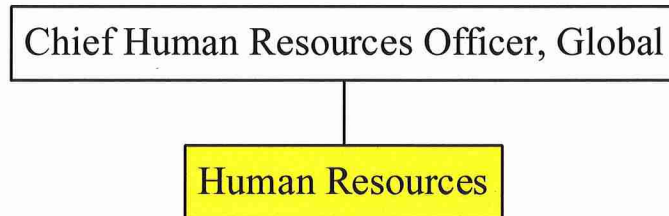
Individual materials that were originally part of a storm skid may be returned. These will appear as a negative amount with no corresponding charge as the storm skid was originally charged as a whole. Examples of materials are sleeves, connectors, tags, etc.

Process for Storm Material Charges Data Review by PM



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 administration**
- (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 Director of Human Resource reviews and updates 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.

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-term 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 and reviews with U.S. Senior Leadership.

Organizational Structure and Responsibilities:

The Human Resource team is globally segmented into a modern delivery platform consisting of Local HR (Generalists); Total Rewards; Talent Acquisition; HR Information Systems, and Shared Services (such as payroll, processing, etc.). Each area establishes global goals for their respective area. Collectively, with input from local Strategic Business Units (SBU), these goals are then adopted by each local SBU with local adjustment by country, region, or company. The Director of Human Resources reports directly to the President and Chief Executive Officer and has a dotted line relationship to the Global Human Resources Organization. Human Resources maintains responsibility for the following utility activities:

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.

- 1) 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
- 2) 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
- 3) Administer and evaluate retirement programs including 401(k) and pension plans
- 4) Maintain the Human Resources information system of record and applicant tracking systems

Employee Relations is responsible for managing, addressing, and resolving employee concerns, as well as maintaining a positive relationship with the bargaining unit.

- 1) Partner with functional areas to provide generalist support and consulting on a broad range of employee issues
- 2) Proactively identify potential employee or labor issues and work to resolve issues with employee or union when applicable
- 3) Ensure proper administration of Company labor agreements

Labor Relations is responsible for maintaining a positive relationship with the bargaining unit and managing the contract and negotiation processes.

- 1) Manage the grievance, arbitration, and negotiation processes

Talent Management is responsible for assessing the people development needs of the organization and creating and executing appropriate training to meet those needs

- 1) Develop performance competencies and structure the performance review process
- 2) Conduct talent dialogues to assess talent strengths and opportunities within each functional area
- 3) Develop the succession plan in conjunction with functional leadership
- 4) Assess developmental needs for individuals and functional areas and recommend, design, and/or deliver trainings to address identified gaps and needed productivity improvements
- 5) Source and on-board new talent and ensure compliance to applicable local, state, and federal regulations and requirements

- 6) Develop and maintain campus recruitment strategies to include intern and co-op programs
- 7) Deliver and maintain employment testing programs to evaluate candidate capability
- 8) Participate in community outreach programs in support of the Company's diversity and inclusion strategy

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 appropriately raised to proper level of authority as required by Company policies.

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.

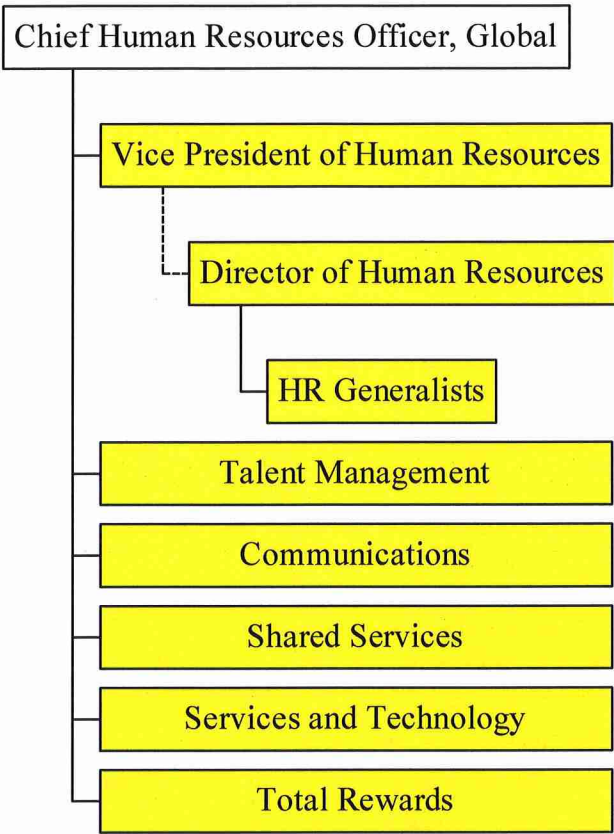
Internal and External Communications:

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 area of the Company. These communications include providing information to all areas of the Company.

External communications will typically involve benefit development, recruiting, and hiring activities.

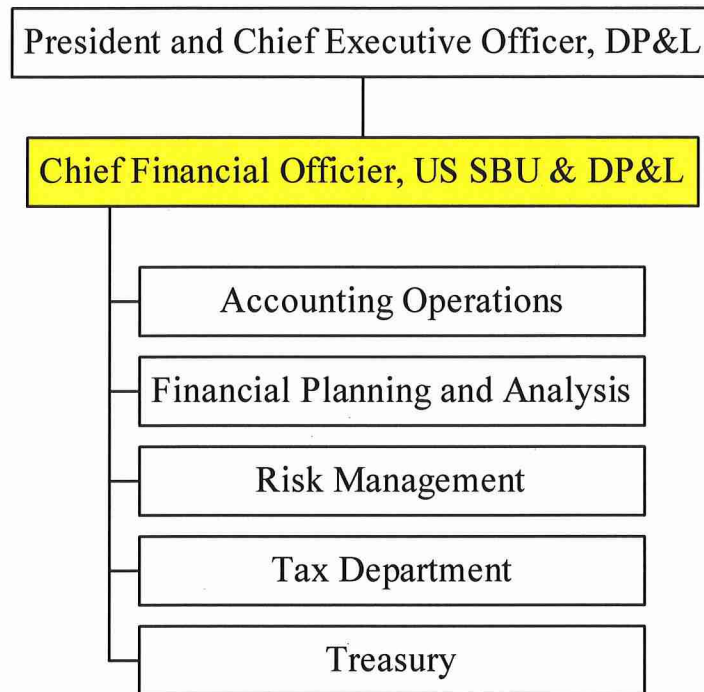
Human Resources – Exhibit 1

Organizational Chart for Human Resources



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
Staff Letter****Policy and Goal Setting:**

The US SBU Controllers Group ("Accounting Operations") 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 has policies that govern US SBU-wide activities such as travel and entertainment, while the US SBU Controller has the authority to approve policies that only impact the Accounting Operations 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 shared site. 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 and strategic 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 General, Operations, Regulatory, Revenue, Fixed Assets Accounting, as well as Financial Reporting, Accounts Payable, Financial Systems and Controls and Technical (dotted line relationship). 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 workload split.

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

- 1) General and Operations 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
 - c) Prepare journal entries related to the operations of generation facilities that are owned jointly with third parties
 - d) Coordinate the capture and monthly allocation of costs incurred by the Service Company on behalf of DP&L
 - e) Prepare monthly occupancy cost allocations to entities who benefit from the use of space owned by DP&L
- 2) 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
- 3) 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
- 4) 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
- 5) 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

- 6) Accounts Payable
 - a) Timely processing of invoice payments
 - b) Compliance with regulations and company policies
- 7) Financial Systems and 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
 - e) Finance digital initiatives and system implementations
- 8) Technical Accounting (dotted line reporting relationship)
 - a) Contract review
 - b) New accounting pronouncement analysis and implementation assistance
 - c) Accounting guidance interpretation as requested
 - d) Derivative accounting

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/DP&L 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 or video 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 are 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, Microsoft Teams video meetings, meetings, and e-mail. Communications typically involve interaction with DP&L's external auditors, vendors and members of the AES Corporate team.

Staff Letter - DP&L's process and controls related to the movement of projects from in progress to in service:

DP&L's policies have been updated to reflect DP&L's movement from Oracle to its SAP enterprise accounting system. The new accounting system allows significant process improvements that help to efficiently move property from in service through to unitization. Additionally, DP&L has improved processes surrounding communication between Fixed Asset Accounting and Project Managers to ensure projects adhere to identified timelines. The Distribution Investment Rider compliance audit by Blue Ridge Consulting Services Inc. in Case No. 19-439-EL-RDR referenced internal audit findings on this topic. These audit findings and recommendations are addressed in Accounting Operations – Exhibit 2.

Staff Letter - DP&L's procedures to review and document the post-closing review of large projects to determine why in-service projects are delayed, with specificity, and what has been done to reduce the number of in-service delays:

The Company reviews the status of projects on a regular basis through its monthly capital status meetings to determine if actions need to be taken to move a project from in construction to in-service and then to unitized. Accounting also follows a quarterly process to document the status of projects, particularly those designated as in-service.

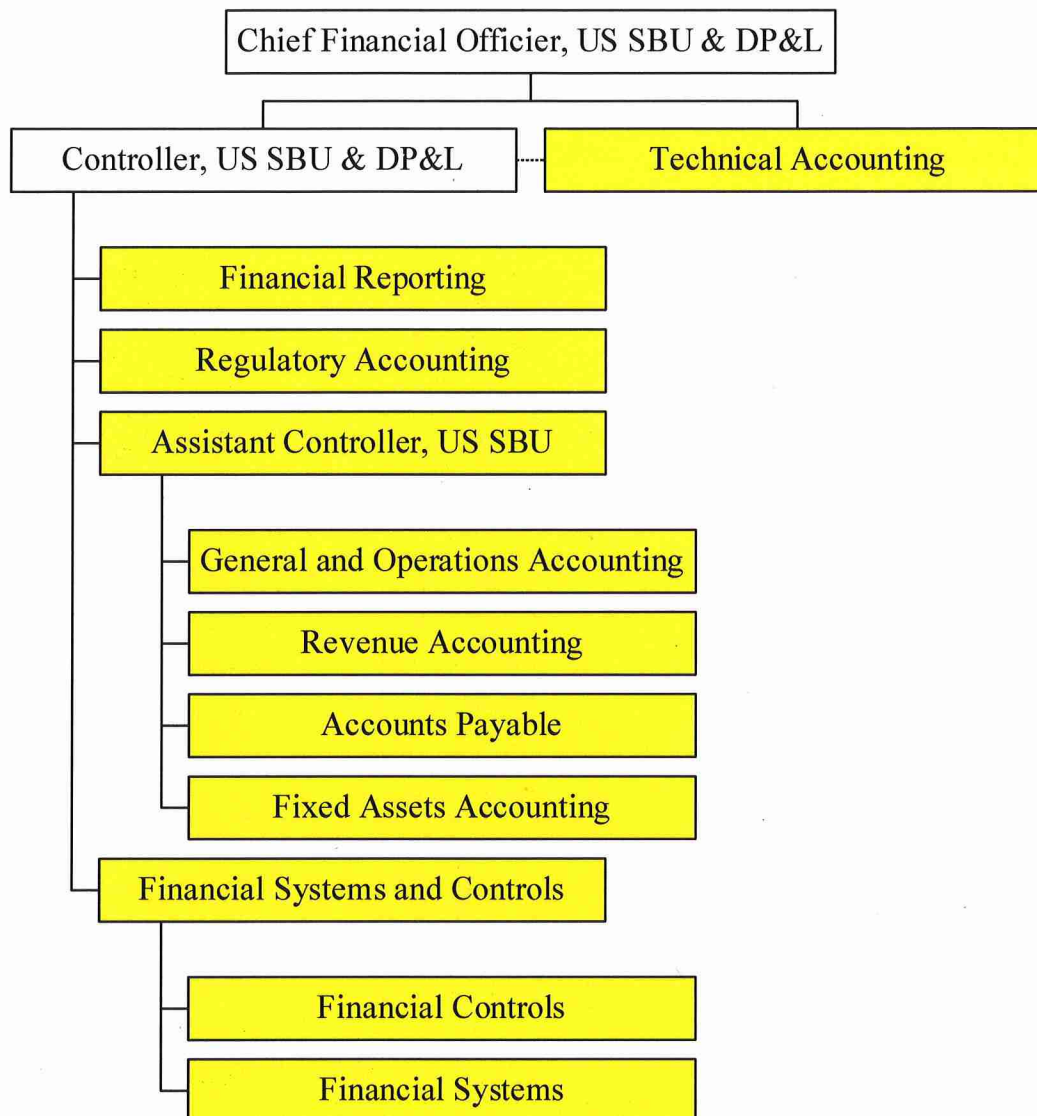
There are many reasons why a project will remain in the 'in-service' state. One of the more common reasons is pole attachments and transfers (commonly referred to as double-wood or two-pole conditions). Historically, if a project included the retirement of a pole with attachments, the project would not be closed and unitized until the pole attachor completed their work and the Company was able to pull the pole stub. This would result in delays to closing the project of months, and in some cases, years.

The Company has made adjustments to its processes to reduce the time a project remains in the 'in-service' state. This includes, but is not limited to, a process focused solely on remediating two-pole conditions through a one-touch approach, moving the handling of pole stubs to separate retirement projects, resources dedicated to communication and coordination with pole attachors (including identifying any expedited needs) and providing project managers with additional

resources to support the project close-out process. Additional detail on this policy can be found in Accounting Operations – Exhibit 3.

Accounting Operations – Exhibit 1

Organizational Chart for Accounting Operations



Accounting Operations – Exhibit 2

Management has taken actions to address the issues outlined in the Blue Ridge Data Request #2 Case No. 19-439-EL-RDR DP&L Distribution and referencing the DPL Capex (CWIP Distribution) Report issued November 13, 2017, as stated in the response below each finding.

T&D Projects Capitalization Process

1. The required transfer of projects from 'in-progress' to 'in-service' was not performed in a consistent, timely manner for all concluded projects.

Recommendations: Operational Area should review the close-out process for damage claim projects in order to ensure that all completed projects are promptly put in service and unitized. Also, a task force should be instituted to clear the backlog of completed projects not in service.

Response: The Operational area ensures that all information and reports are completed in Stakeout, as well as material, invoices, and remaining costs are posted to SAP before notifying the Damage Claims department to initiate billings. The project in SAP will be analyzed and billed by the Damage Claims department and after the completion of the invoice, Damage Claims department will notify the Project Manager (PM) of completion. The PM will then Technically Complete (TECO) the WBS in SAP which moves the project to in-service (FERC 106) and has 120 days to move the WBS from TECO to Closed Status in SAP so that it can be unitized.

2. Project managers should improve the monitoring process of ongoing projects in order to ensure that all completed projects are timely identified and close-out. Also, operational management should reinforce the importance of providing Fixed Assets Accounting with timely and accurate information on projects status, in order to ensure correct accounting treatment of each project.

Response: Fixed Assets Accounting completes a quarterly detailed CWIP report for Operational Management to review and to provide input on project status and completion. Fixed Assets follows up with any questions regarding projects with extended activity and the action plan for completion.

3. Projects on hold must be reviewed by the operational area in order to ensure that management is committed to funding the entire project. Also, management must be able to assert that the combination of achieved and future milestones indicates a greater than 75% likelihood of success. In case there is no funding allocated, the operational team should notify Fixed Assets Accounting to take the proper action.

Response: The Operational Area analyzes the capital spend on each project through monthly review meetings with Management, as well as through the quarterly 3.CAP.3

review reports sent by Fixed Assets. If projects do not meet the 75% criteria and will not continue, then any dollars spent to date will be transferred to O&M and cancelled.

4. Fixed Assets Accounting should improve monitoring controls of projects in progress, including but not limited to inquiring of aged projects without recent charges and unclear status provided by Project Managers, and projects "On hold" for extended periods of time.

Response: Fixed Assets reviews through the quarterly 3.CAP.3 report as well as a Power Plan reports that help with reviewing projects past their in-service dates allowing for Fixed Asset to work closely with the Project Managers to address the projects in question.

5. Fixed Assets Accounting should review and correct the projects that were put in service in duplicity. Going forward, should develop a process to ensure that the projects manually put "In service" are not already automatically unitized.

Response: The duplication issue has been eliminated due to the process being automated with the implementation of accounting systems, SAP and Power Plan, in April 2019.

Accounting Operations – Exhibit 3

DP&L Transmission & Distribution Work Order Closing Review Policy

This policy provides project managers, as well as others responsible for projects, guidance on the process for reviewing and submitting the proper project information to the Fixed Asset Accounting group for closing and unitization.

Projects estimated in Stakeout are reviewed by the project manager and closed to Plant within 90 days after the work has been completed. SAP initiated work orders, including blanket projects for new services, multiple taxing location distribution projects, transmission and substation projects, and other miscellaneous general plant (e.g. real estate, transportation, IT, etc.) projects are reviewed by the project manager and closed by the Fixed Asset Accounting department within 120 days of project completion.

The amount of review work that should be completed in preparation for closing a work order depends on the cost and complexity of the project. More time should be spent reviewing a project of significant scope and/or cost than one of lesser amount and/or complexity. A guideline for the review of projects with estimated and actual costs below \$25,000 is outlined in section I, below. Some additional review procedures for projects exceeding \$25,000 are then described in section II.

I. Projects with actual and estimated costs of \$25,000 or less:

- The project manager should verify that the project is properly approved in accordance with the Company's expenditure authorization policy at that time. The project should have appropriate authorizations within StakeOut or SAP (non-StakeOut projects). Where applicable for any projects closed prior to the Company's implementation of SAP on 4/1/2019, the signature of the approver must appear on any manual work order forms or the Project Expenditure Authorizations (PEA). If the project was engineered in Stakeout, the electronic ID of the approver must be populated.
- Review the work order scope as described on the manual work order form, PEA or the Stakeout Cost Estimate Summary to determine whether the project involves construction and/or retirement. When the project involves construction, there must be at least one unit of property installed. When the project involves the replacement of units of property, there should be units of property being retired (exceptions include projects involving two-pole conditions where the removal will be completed at a later date on a retirement-only project). When the job only involves the removal of units of property, there should be no cost charged to construction. Any contributions in aid to construction (CIAC) are noted on the Invoicing tab in Stakeout, on the manual work order form or PEA for Oracle projects (pre-SAP), or as a credit to the project for all other SAP projects. If billing is involved with the job, determine if the money has been collected or if the customer has been invoiced. Document type DR in SAP is the invoice that is used to charge the collection of taxable contributions.
- Display/print the T-code CJI3 in SAP for the project details (WBS detail). Review the cost elements and/or general ledger entries with charges for reasonableness in light of the requirements above. Common cost elements assigned to a project include:

- Salaries & Wages (management and union, including overtime)
- Engineering Consulting
- Non-Stock Supplies
- Supplies Purchases
- A&G Overheads
- S&E Overheads
- Benefits Overheads
- AFUDC

Stakeout Projects (Capital)

- Compare the estimated units of property listed in Stakeout to the installed units on the updated construction prints from the field. In Stakeout the units of property will be listed on the Property Accounting Records Listing. If the actual installed units vary from the original plan, correct the units in Stakeout before closing the project. If there is any question as to the units of property actually installed, run the CJI3 report to confirm materials charged and verify property units. This will list the specific material items charged from stores to the project.
- If there are no units of property installed or removed, then it cannot be considered a capital project and the accumulated project cost must be transferred to the appropriate account number and the capital project cancelled in Stakeout, SAP, and PowerPlan.
- To review cost, Stakeout project users should print the T-code CJI3 from SAP to determine the total cost of the project (CJI3 shows actual costs as well as credits such as CIAC). This report will summarize the actual costs charged to the project by cost category. Review the report for reasonableness as described by the following. For a construction project there should be some labor (internal and/or contractor), material, transportation, and overheads charged. If a contractor performs the job or the materials are purchased and charged directly to the project, the CJI3 report in SAP should indicate the amount of cost under supplier invoices.
- Compare the total actual cost incurred as shown on the CJI3 report to the estimated cost on the approved Stakeout Cost Estimating Summary for reasonableness. If the estimate and the actual costs are in-line, no further review of detail charges is needed. When the project contains unusual or unreasonable charges, initiate an investigation to determine if a possible correction between capital and expense is required. Unreasonable deviation is typically considered greater than 10%, however, there could be exceptions.
 - 1.
- The person reviewing the cost should print and attach the CJI3 report, along with signing the Service Operations – StakeOut Projects - Close-Out Sign-Off to include in the project folder.
- Review the Stakeout Project Information screen to make certain an accurate project in-service date has been entered. This is found on the Construction Line tab (overhead construction complete and/or underground construction complete dates).

SAP Initiated Projects (Capital)

- For non-StakeOut projects when using the manual work order form or a PEA, the units of property should be written on the front of the document or attached to the documents. If items were issued from DP&L's storeroom, run the CJI3 report with DPL_MATLRPT layout from SAP. This will list the specific material items charged from stores to the project

(this report will not list items purchased from outside sources).

- If there are no units of property installed or removed, then it cannot be considered a capital project and the accumulated project cost must be transferred to the appropriate account number and the capital project cancelled in SAP and PowerPlan.
- Compare the total actual cost incurred as shown on the CJI3 report from SAP to the estimated cost on the approved manual work order form or PEA for reasonableness. If the estimate and the actual costs are in-line, no further review of detail charges is needed. When the project contains unusual or unreasonable charges, initiate an investigation to determine if a possible correction between capital and expense is required.
- The person reviewing the cost should print and attach the CJI3 report, along with signing the Service Operations – SAP/Oracle Initiated Projects - Close-Out Sign-Off to include in the project folder.
- The in-service date should be written on the manual work order or PEA along with a signature of the project manager verifying the in-service date.
- The approved manual work order or PEA with property units, in-service date and signature verifying the service date, along with the Service Operations - Oracle Initiated Projects - Close-Out Sign-Off are sent to the Accounting Department where they will unitize/close the work order.

II. Projects with estimated or actual cost in excess of \$25,000

- Follow all steps as outlined for projects less than \$25,000
- Throughout the construction period the project manager should monitor the actual costs to the approved budget as shown on the CJI3 report (alternatively, report CN41N can be run to show Actual vs. Budget dollars by WBS). As soon as the Project Manager is aware that the project will exceed the 15% variance (due to scope change, construction related issues, etc) they must submit a revised budget amount in SAP and/or StakeOut and submit the project for re-authorization (project goes through its original approval steps).
- If the actual cost varies from the estimate by more than 15%, the approver(s) will be notified and the variance approved via project re-approval within SAP and/or StakeOut. For projects that were originally approved with a PEA and completed prior to the implementation of SAP, and the PEA varies from the estimate by + 15%, a supplemental PEA needs to be approved. If the amount varies from the estimate by -15% then the PEA Under Spend form must be completed. When the total cost of the project exceeds the expenditure authorization of the original approver, the project will be re-approved based on the actual level of expenditure, per Company expenditure authorization policy at that time.
- If there are significant cost variances between the estimated and actual cost by category, investigate these differences by running the appropriate detail SAP report (most commonly CJI3) for the category of cost in question.
- It may be necessary to make accounting corrections in SAP depending on the materiality of any errors identified during the closing review. Requests for any corrections should be made to the Fixed Asset Accounting group.

- For projects in excess of \$500K, project managers should follow the instructions and complete the Non-StakeOut Project Close-Out Checklist within 30 days of construction completion. The report needs to include the in-service date and total costs so that Fixed Asset Accounting can transfer the dollars out of CWIP (construction work in progress) into In-Service. A complete list of assets and taxing locations must be submitted with closing documentation.

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 Chief Financial Officer.

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 Chief Financial Officer.

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 on 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:

Financial Planning and Analysis consists of 1 manager and 2 analysts who are led by the Manager of Financial Planning and Analysis reporting to the Chief Financial Officer. 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 appropriately 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.

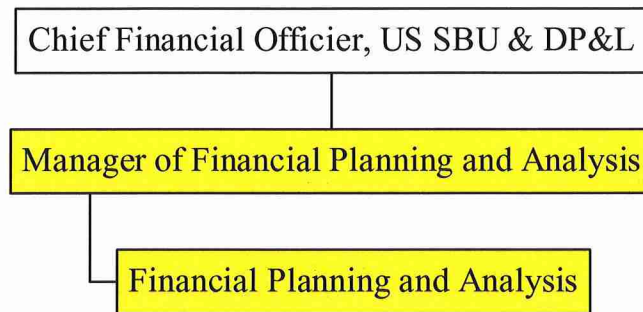
Assumptions and analysis are reviewed by the Manager of Financial Planning and Analysis for reasonableness and consistency in theory application.

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:
Risk Management

SFR Reference
(B)(9)(b)(vii) Risk management

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.

Strategic and Long-Range Planning:

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 through the Market Management Strategy (MMS).

Organizational Structure and Responsibilities:

The Risk Management function falls under the control of the US SBU CFO with a dotted line report to the Vice President of Risk at AES Corporate. While not a direct reporting relationship, frequent communication and consultation occurs with AES Corporate Risk Management Oversight Committee and the US SBU RMC. The Director of Risk Management has one direct report in Risk. There are no other areas that report to Risk Management.

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:

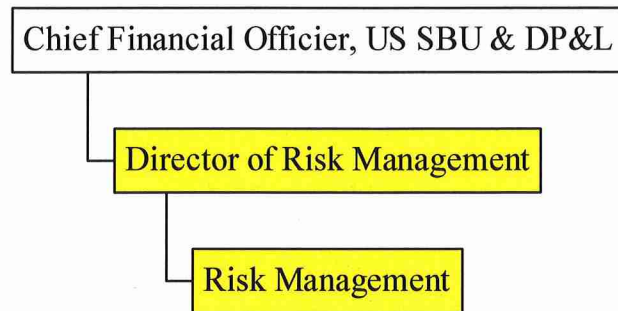
- 1) Routine and adhoc risk reporting
- 2) Monthly RMC meetings
- 3) Risk updates to Corporate Risk Oversight Committee
- 4) Interaction with commercial team members and other key stakeholders regarding the company's evolving risk profile, drivers of change, and preparation of a market risk management strategy

Decision-Making and Control:

The decision-making process for commercial transactions is governed by the risk management 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 an RMC vote must receive majority approval, with certain members of the RMC having veto rights.

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 and attending an annual safety awareness day.

The goal setting process for the Tax Department is a joint effort between the AES Chief Tax Officer, US SBU 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) Comply with all applicable Federal, State, and local tax laws
- 2) Ensure filing of all returns and payments on a timely basis
- 3) Assure that DP&L's tax accounting practices are in accordance with the respective regulatory agencies' requirements
- 4) Support DP&L's position in regulatory initiatives
- 5) Participate in the development of tax legislation
- 6) Provide tax assistance as may be requested by others in the organization

Strategic and Long-Range Planning:

AES' 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 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 Managing Director – US Tax Reporting and Corporate Planning. The Department's functions are: (1) Tax accounting and regulatory compliance; (2) Tax compliance (including US Federal income tax, 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 appropriately 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.

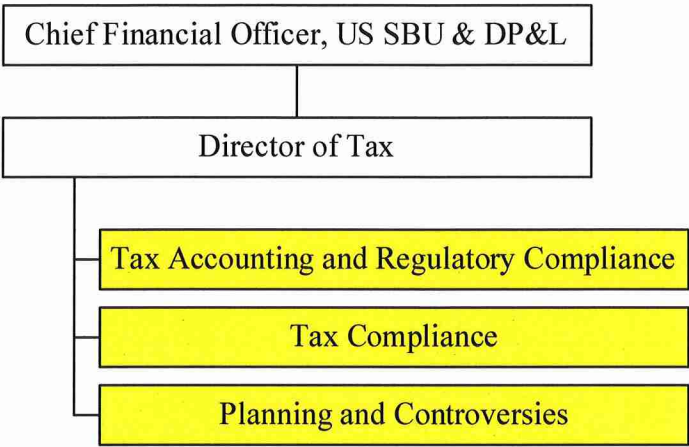
Periodic staff meetings are held by the AES Chief Tax Officer as well as by the US SBU Director of Tax. These meetings provide a forum for discussing commercial events that affect tax operations, updates on projects, as well as discussions regarding priorities and practices. Furthermore, Tax Department 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 the policies governing the financial functions at US Services are ultimately the responsibility of the Company's CFO, who is required to protect all the financial assets and manage 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 which 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

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 (manage to a target capitalization level and appropriately balance debt maturity profiles with cost of debt alternatives)
- 2) Optimize liquidity profile (maintain adequate working capital and liquidity backstops to support collateral calls, unexpected events and enhance overall credit profile)
- 3) Efficiently invest/manage financial assets (allocate capital in the most productive manner whether it be through reinvestment, debt repayment, distribution to DPL Inc, or short-term investment)
- 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 receipts, investments 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

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.

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 or indirectly 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.

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 Chief Financial Officer 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 key performance indicators 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.

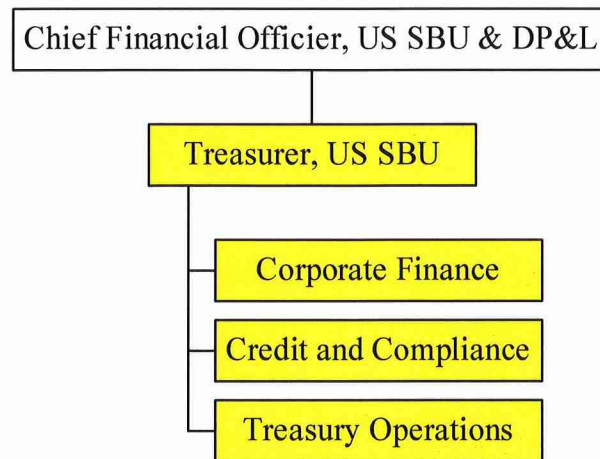
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels (formal and informal) including; in-person/virtual 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, trustees, and others in order to conduct business on behalf of and for the benefit of DP&L.

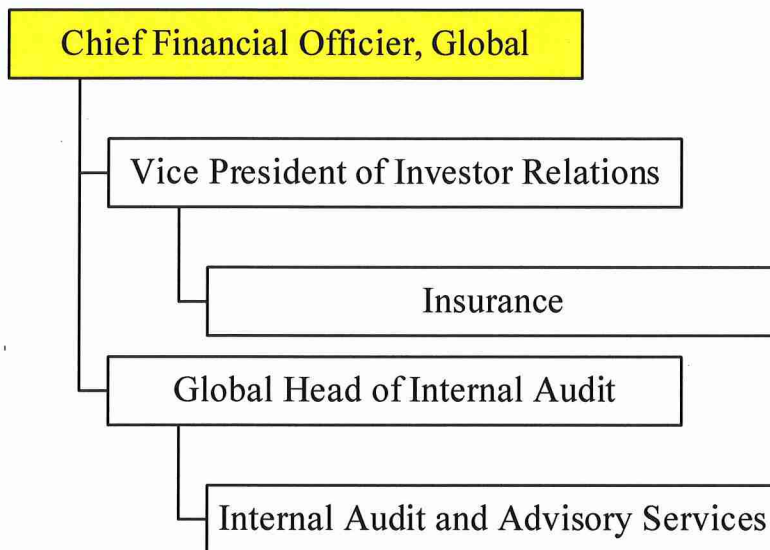
Treasury – Exhibit 1

Organizational chart for Treasury



Office of Chief Financial Officer, Global

Global Finance is responsible for the ensuring that AES subsidiaries have the financial security needed to support their individual primary mission of providing reliable and affordable electric service. The functions provided by Global Finance are described in detail in the following sections.



Functional Area:**Insurance****SFR Reference****(B)(9)(e)(ii) Insurance****Policy and Goal Setting:**

The 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.

Insurance typically centers on obtaining the most favorable risk transfer terms at the most favorable cost.

Strategic and Long-Range Planning:

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 Insurance function falls under the control of the AES CFO. While not a direct reporting relationship, frequent communication and consultation occurs with US SBU CFO.

Insurance is responsible for protecting the company's assets from fortuitous loss while simultaneously ensuring, to the greatest extent possible, a predictable level of cash flow and expenses. This is accomplished through:

- 1) Continual evaluation of insurable risks facing the organization
- 2) The purchase of traditional insurance
- 3) Diligent management of DPL's captive insurance company, Miami Valley Insurance Company
- 4) Contractual risk management/risk transfer
- 5) Advocating strong loss control processes (specific to both liability and property exposures)
- 6) Development of programs geared towards reducing the exposure to loss

The organizational chart for Insurance is included as Insurance – Exhibit 1.

Decision-Making and Control:

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, an annual loss reserve study is 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.

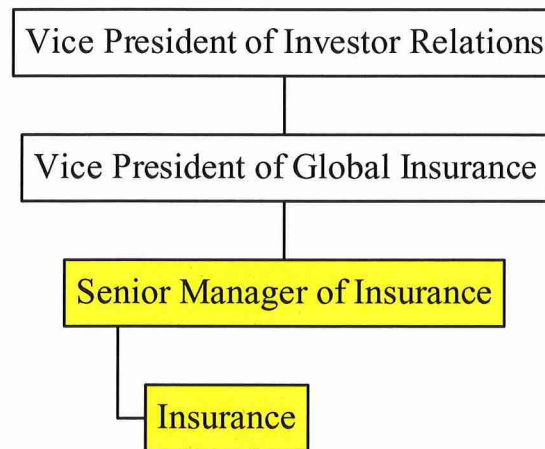
Internal and External Communications:

Internal communications are accomplished through a variety of communication channels including; Microsoft Teams, 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; Microsoft Teams, Zoom, 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.

Insurance – Exhibit 1

Organizational chart for Insurance



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 advisory services designed to add value, improve DP&L's operations, and ensure compliance with internal policies 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 scope of work of Internal Audit and Advisory Services group is to determine whether AES's risk management, internal controls, and governance processes, as designed and represented by management, is adequate and functioning in a manner to ensure:

- 1) Significant financial, managerial, and operating information is accurate, reliable and timely
- 2) Employee actions are compliant with policies, standards, procedures and applicable laws and regulations
- 3) Company resources are acquired economically, used efficiently, and adequately protected
- 4) Quality and continuous improvement are fostered in AES's control process
- 5) Risks are appropriately identified and managed in a timely manner
- 6) Interaction with the governance processes across all SBU's occurs as needed
- 7) Company programs, plans and objectives are achieved in an efficient and economical manner

- 8) Significant legislature or regulatory issues affecting AES are recognized and addressed appropriately

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 Financial Audit Committee and administratively to the AES Chief Financial 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 AES CAE and the US SBU Chief Financial Officer.

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 Financial Audit Committee for review and approval. Any significant modifications or updates to the audit plan following the initial approval will also be presented to the Financial Audit Committee for review and comment.
- 2) Execute the approved annual audit plan including special tasks or projects requested by management and the Financial Audit Committee.
- 3) Oversee the company testing of internal controls to support management's annual assertions on the effectiveness of internal control over financial reporting as required by 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 requirements of the Internal Audit and Advisory Services Charter.
- 5) Evaluate and assess significant new or changing services, processes, operations, and controls that coincide with development, implementation, and/or expansion of a function or business.
- 6) Issue periodic reports to the Financial Audit Committee and management summarizing results of audit activities.
- 7) Inform the Financial Audit Committee of emerging trends and successful practices in internal auditing.

- 8) At the request of management and/or the Financial Audit Committee, assist in the investigation of significant suspected fraudulent activities within AES. Notification of the results of these investigations shall be the sole responsibility of the Vice President of Ethics and Compliance. All involvement in investigations must be approved in advance by the CAE and the Chief Compliance Officer
- 9) Establish and maintain a quality assurance and improvement program to ensure internal audit responsibilities are performed in an effective and efficient manner

Opportunities for improving management control, profitability, and DP&L/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 DP&L/AES functions, records, property and personnel
- 2) Have full and free access to the Financial Audit Committee
- 3) Allocate resources, set frequencies, identify and execute projects and determine scopes of work to accomplish audit objectives
- 4) Receive full assistance from DP&L/AES personnel

The CAE, Directors and staff of the Internal Audit and Advisory Services department are not authorized to:

- 1) Perform any operational duties for AES or its affiliates
- 2) Perform searches of electronic mail without prior approval from the AES General Counsel
- 3) Initiate or approve accounting transactions external to Internal Audit and Advisory Services
- 4) Direct the activities of any AES employee not employed by Internal Audit and Advisory Services department, 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 guidelines and responsibilities for audit and advisory projects performed during an audit year. Standard operating procedures have been developed for guidance around conduct 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

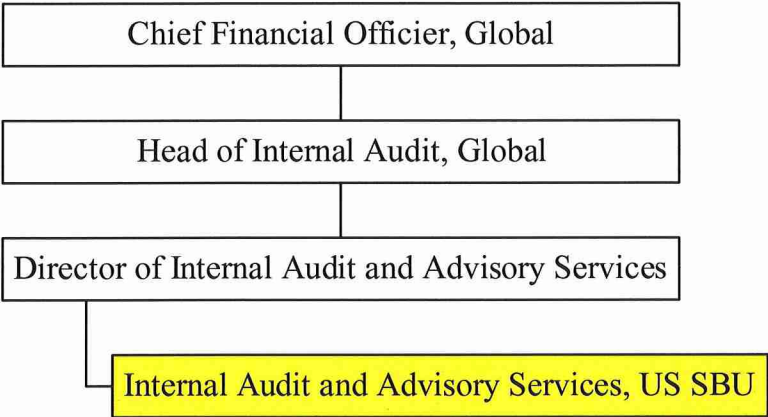
Further guidance is also available on sample selection for audit tests performed, materiality levels, and report ratings/conclusions.

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 provides periodic updates to the Financial Audit Committee on current audits.

Internal Audit and Advisory Services – Exhibit 1

Organizational Chart for Internal Audit and Advisory Services



This foregoing document was electronically filed with the Public Utilities

Commission of Ohio Docketing Information System on

11/30/2020 1:54:20 PM

in

Case No(s). 20-1651-EL-AIR, 20-1652-EL-AAM, 20-1653-EL-ATA

Summary: Application Book I - Application and Supplemental, Volume 3 of 11 electronically filed by Mr. Jeffrey S Sharkey on behalf of The Dayton Power and Light Company