State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Solicitation

NUMBER	PAGE
FAR140001	1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
GUY NISBET
304-558-2596

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
DEPARTMENT OF ADMINISTRATION
FINANCIAL ACCOUNTING AND
REPORTING SECTION
2101 WASHINGTON ST E
CHARLESTON, WV
25305-1510 304-558-4083

DATE PRINTED
04/18/2014

BID OPENING DATE: 05/15/2014 BID OPENING TIME 1:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
	ADDENDUM NO.02					
	ADDENDUM ISSUED TO PUBLISH AND DISTRIBUTE THE ATTACHED INFORMATION TO THE VENDOR COMMUNITY.					
0001	1	LS		946-20		
	AUDIT OF STATE CAFR					
	****** THIS IS THE END OF RFQ FAR140001 ****** TOTAL:					

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO SOLICITATION, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

SOLICITATION NUMBER: FAR140001
Addendum Number: No. 02

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[✓] Other

Description of Modification to Solicitation:

1. Addendum issued to distribute copies of the 2013 State Rail's audit and the 2013 OT SOC 1 Report to the vendor community.

2. No other Changes.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

WEST VIRGINIA STATE RAIL AUTHORITY

A COMPONENT UNIT OF THE STATE OF WEST VIRGINIA
AND THE WEST VIRGINIA DEPARTMENT OF TRANSPORTATION

FINANCIAL STATEMENTS WITH ADDITIONAL INFORMATION

YEAR ENDED JUNE 30, 2013

AND

INDEPENDENT AUDITOR'S REPORT

TABLE OF CONTENTS

Suttle & Stalnaker PLLC
CERTIFIED PUBLIC ACCOUNTANTS

INDEPENDENT AUDITOR'S REPORT

To the Members
West Virginia State Rail Authority
Moorefield, West Virginia

Report on the Financial Statements

We have audited the accompanying financial statements of the West Virginia State Rail Authority (the Authority), a component unit of the State of West Virginia Department of Transportation, as of and for the year ended June 30, 2013, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements as listed in the table of contents.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the business-type activities of the Authority as of June 30, 2013 and 2012, and the respective changes in financial position and, where applicable cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America.

Emphasis of Matter

As described in Note 1 to the financial statements, in fiscal year 2013, the Authority adopted new accounting guidance, GASB Statement No. 63, *Financial Reporting of Deferred Outflows of Resources, Deferred Inflows of Resources, and Net Position,* GASB Statement No. 65, *Items Previously Reported as Assets and Liabilities,* and GASB Statement No. 66, *Technical Corrections -2012- an amendment of GASB Statement No. 10 and No. 62.* Our opinion is not modified with respect to this matter.

Other Matters

Required Supplementary Information

Accounting principles generally accepted in the United States of America require that the management's discussion and analysis and budgetary comparison information on pages 5-10 be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the Governmental Accounting Standards Board, who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Reporting Required by *Government Auditing Standards*

In accordance with *Government Auditing Standards*, we have also issued our report dated October 22, 2013, on our consideration of the Authority's internal control over financial reporting and on our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements and other matters. The purpose of that report is to describe the scope of our testing of internal control over financial reporting and compliance and the results of that testing, and not to provide an opinion on internal control over financial reporting or on compliance.

That report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering Authority's internal control over financial reporting and compliance.

Suttle & Stalnaker, PLLC

Charleston, West Virginia
October 22, 2013

WEST VIRGINIA STATE RAIL AUTHORITY
MANAGEMENT'S DISCUSSION AND ANALYSIS
YEAR ENDED JUNE 30, 2013

The management of the West Virginia State Rail Authority (the Authority) offers readers of our financial statements the following narrative overview and analysis of our financial activities for the year ended June 30, 2013. Please read it in conjunction with the Authority's basic financial statements and notes to the financial statements which follow this section.

FINANCIAL HIGHLIGHTS

- The Authority's net position increased by approximately $826 thousand as a result of this year's operations. This was due to continual capital improvement projects and upgrades to both the South Branch Valley Railroad (SBVR) and the West Virginia Central Railroad (WVCR) funded through legislative appropriation and freight revenues.

- Operating expenses increased by approximately $970 thousand during the year ended June 30, 2013, and operating revenues decreased by approximately $412 thousand. This resulted in an operating loss increase of approximately $1.4 million compared to the year ended June 30, 2012. Operating expenses increased due to expenses incurred for the development of the WV State Rail Plan. Salaries and benefits, car hire, diesel fuel, and liability and property insurance rates are normally the largest operating expenses but rail planning was included in expenses for the year ended June 30, 2013. Freight revenue decreased due to a decrease in freight cars of 200 total cars. Pilgrim's Pride decreased by 310 cars because of the availability of local corn being shipped by trucks. This trend is not expected to continue. Allegheny Wood and Appalachian Railcar were down slightly while Greer Lime showed an increase of 132 revenue cars for the year.

- Non-operating revenues (expenses) were approximately $3.7 million in the year ended June 30, 2013 compared to non-operating revenues (expenses) of approximately $2.3 million in the year ended June 30, 2012. The increase in total non-operating revenues (expenses) of approximately $1.4 million was due to an increase in intergovernmental revenue and federal revenue.

- The Authority completed approximately $3.1 million in capital improvements in the year ended June 30, 2013, including approximately $731 thousand for SBVR track, approximately $191 thousand for SBVR equipment, approximately $35 thousand for SBVR locomotives, approximately $1.7 million for WVCR track and approximately $457 thousand in land purchases.

OVERVIEW OF THE FINANCIAL STATEMENTS

This annual report includes management's discussion and analysis report, the independent auditors' report and the basic financial statements of the Authority. The financial statements also include notes that explain in more detail some of the information in the financial statements.

The financial statements of the Authority report information using accounting methods similar to those used by private sector companies. These statements offer short and long-term financial information about its activities. The Statement of Net Position includes all of the Authority's assets and liabilities and provides information about the investments in resources (assets) and the obligations to creditors (liabilities). It also provides the basis for evaluating the capital structure of the Authority and assessing the liquidity and financial flexibility of the Authority.

All of the current year's revenues and expenses are accounted for in the Statement of Revenues, Expenses, and Changes in Net Position. This statement measures the success of the Authority's operations over the past year and can be used to determine whether the Authority's costs are recovered from revenues and how much of the cost is supplemented by appropriations from the State of West Virginia.

The final required financial statement is the Statement of Cash Flows. This statement reports cash receipts, cash payments, and net changes in cash resulting from operating, investing, and financing activities. It provides answers to such questions as where did cash come from, what was cash used for, and what was the change in the cash balance during the reporting period.

CONDENSED FINANCIAL STATEMENTS

Condensed financial information from the Statements of Net Position and Statements of Revenues, Expenses and Changes in Net Position for the years ended June 30, 2013 and 2012 are as follows:

Condensed Statement of Net Position

	2013	2012	Variance
Current assets	$ 7,126,142	$ 6,057,849	$ 1,068,293
Capital assets, net	38,764,065	37,488,489	1,275,576
Total assets	45,890,207	43,546,338	2,343,869
Current liabilities	1,704,105	190,435	1,513,670
Noncurrent liabilities	541,161	536,782	4,379
Total liabilities	2,245,266	727,217	1,518,049
Net position			
Invested in capital assets, net of related debt	38,764,065	37,488,489	1,275,576
Unrestricted	4,880,876	5,330,632	(449,756)
Total net position	$ 43,644,941	$ 42,819,121	$ 825,820

Condensed Statement of Revenues, Expenses, and Changes in Net Position

	2013	2012	Variance
Operating revenues			
Freight	$ 2,269,323	$ 2,300,674	$ (31,351)
Miscellaneous	208,542	589,294	(380,752)
Total operating revenues	2,477,865	2,889,968	(412,103)
Depreciation expense	1,773,843	1,692,694	81,149
Other operating expenses	3,590,324	2,701,407	888,917
Total operating expenses	5,364,167	4,394,101	970,066
Operating loss	(2,886,302)	(1,504,133)	(1,382,169)
Non-operating revenues (expenses)	3,712,122	2,300,368	1,411,754
Change in net position	825,820	796,235	29,585
Total net position - beginning	42,819,121	42,022,886	796,235
Total net position - ending	$ 43,644,941	$ 42,819,121	$ 825,820

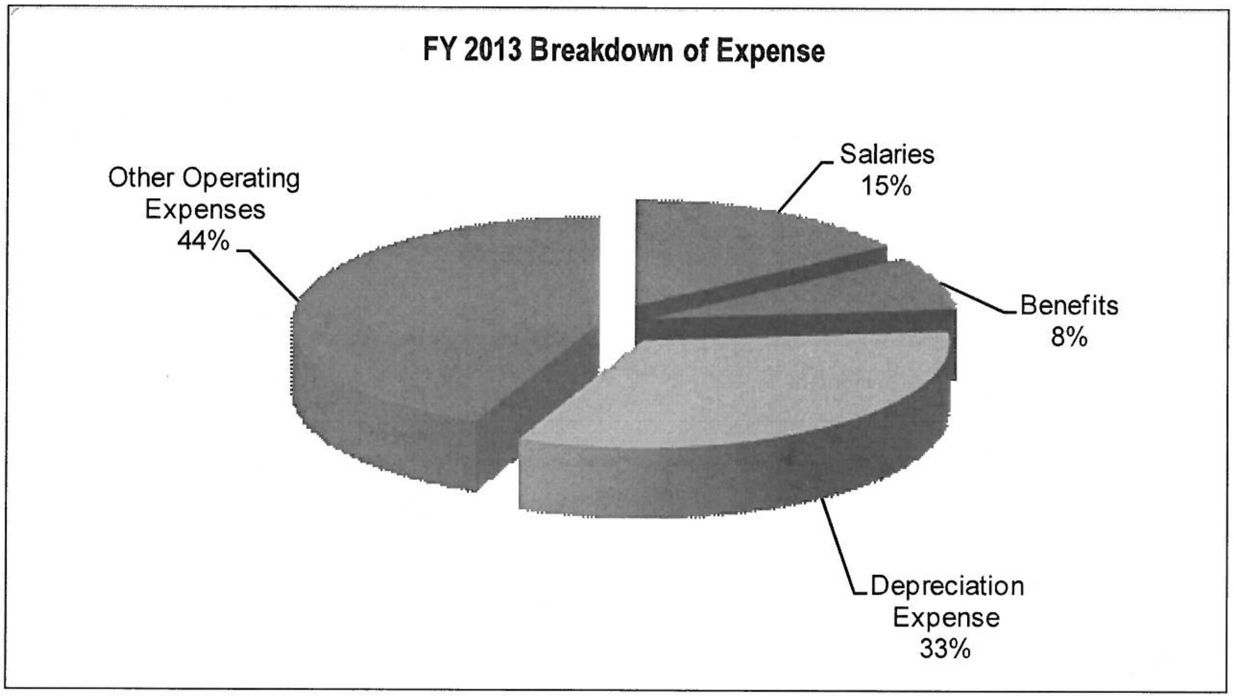
FINANCIAL ANALYSIS

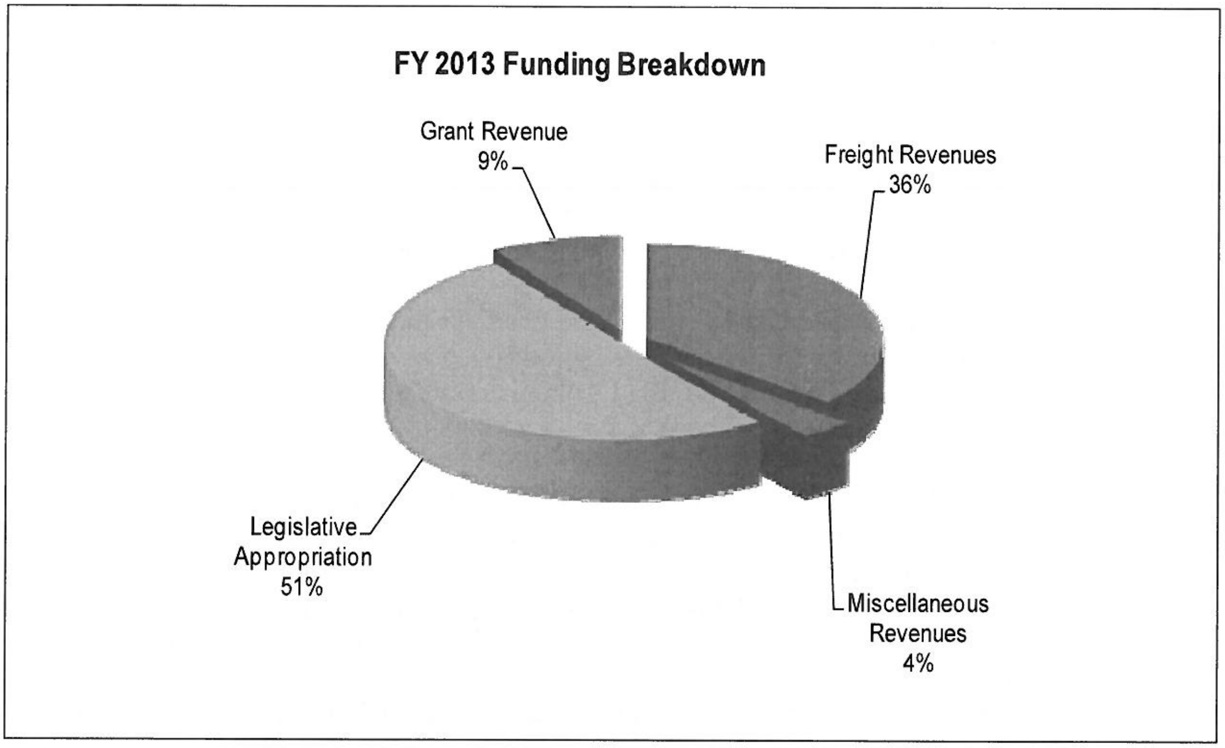
- The Authority's budget for the fiscal year ended June 30, 2013 consisted of funds received from the State of West Virginia General Fund, operating revenues from SBVR, revenues from the operator of the WVCR, federal drawdowns from an FRA grant and miscellaneous revenues received from the leases and licenses on railroad right-of-ways.

- The Authority received an approximate $3.2 million appropriation from the general fund of the State of West Virginia for capital improvement projects and maintenance projects on the SBVR and WVCR, upkeep of the Maryland Rail Commuter (MARC) train stations in the eastern panhandle, and the general operation of the Authority. This appropriation is about 51% of the total funds received. Funds will continue to be utilized for capital improvements and maintenance costs on the SBVR and WVCR in order to safely maintain the condition of both railroads. The SRA also earned approximately $559 thousand from a Federal Railroad Administration grant that was used for the partial payment of the preparation of the WV State Rail Plan.

- Freight revenue of approximately $2.3 million was earned from the operations of the SBVR, which was in line with the year ended June 30, 2013 budgeted projections. Miscellaneous revenues of approximately $209 thousand were earned in addition to the freight revenue. The miscellaneous revenue is made up of right-of-way leases on the SBVR and WVCR and income received from the excursion train operators. This revenue is used to help pay the operating expenses of the SBVR. Total operating revenues decreased by approximately 14% in the fiscal year ended June 30, 2013. Miscellaneous revenue decreased by 65% in the fiscal year ended June 30, 2013. This was due revenues received from the sale of scrap surplus that did not occur in 2013.

The following graphs provide a visual representation of the funding (revenue and other income sources) and expenditures for the fiscal year ended June 30, 2013.





CAPITAL ASSETS

The Authority's net capital assets as of June 30, 2013 and 2012 amounted to approximately $38.8 million and approximately $37.5 million, respectively. This investment in capital assets includes land, buildings, railroad infrastructure, rail cars and equipment.

The Authority primarily acquires its assets with proceeds from the general fund appropriation from the State of West Virginia. Rehabilitation and improvements to the SBVR and WVCR are part of the Authority's capital improvement program.

Capital asset additions for the years ended June 30, 2013 and 2012 are as follows:

	2013	2012
Land	$ 457,500	$ -
Work equipment	190,642	111,769
Locomotive, freight and passenger cars	34,819	62,250
Railroad infrastructure	2,434,869	1,744,974
Total	$ 3,117,830	$ 1,918,993

Readers interested in more detailed information regarding capital assets should review the accompanying notes to the financial statements.

ECONOMIC FACTORS AND NEXT YEAR'S BUDGET

The Authority's year ending June 30, 2014 budget includes approximately $4.2 million from the State of West Virginia and approximately $2.5 million from projected freight revenue. This funding will be used to complete capital improvement and rehabilitation projects on the SBVR and WVCR. The funding from the State of West Virginia includes approximately $687 thousand (50/50) match for a federal grant for the Authority to develop a State Rail Plan and approximately $1.1 million in appropriated funds for projects underway but not completed in 2013.

The SBVR's track structure has improved significantly over the past twelve years. By establishing a long-term capital improvement program, the Authority has been able to raise the weight restriction on railcars and improve safety of the operation. New locomotives have been added to the fleet to ensure that the SBVR can move traffic in a reliable and timely manner. This is particularly important in handling unit trains for the Pilgrim's Pride feed mill in Moorefield. Pilgrim's Pride is the largest employer in the South Branch Valley, so it is vital that the Authority continue to upgrade the rail infrastructure and maintain the track to promote the economic success of the area it serves. The SBVR capital improvement projects planned for the fiscal year ending June 30, 2014 include continuing to upgrade and repair bridges, replacing cross ties, spreading ballast, surface, weld jointed rail at some locations, upgrading the Moorefield yard tracks and adding an addition to the shop building.

The capital improvement projects planned on the WVCR for the fiscal year ending June 30, 2014 include replacing cross ties, spreading ballast, surface, replacing culverts, and switch tie replacement in the South Elkins yard. This railroad has completed fourteen years of operations and continues to be a strong economic factor to the areas that it serves.

The Authority will continue to maintain commuter facilities at Harpers Ferry, Duffield's, and Martinsburg for the Maryland Rail Commuter (MARC) train service. This offers West Virginia citizens in the eastern panhandle the advantage of using commuter train service to Washington, DC.

REQUESTS FOR INFORMATION

This financial report is designed to provide an overview of the finances of the Authority for those with an interest in this organization. Questions concerning any of the information provided in this report or requests for additional financial information should be addressed to the West Virginia State Rail Authority at 120 Water Plant Drive, Moorefield, West Virginia, 26836.

WEST VIRGINIA STATE RAIL AUTHORITY
STATEMENT OF NET POSITION
JUNE 30, 2013

ASSETS		
Current assets		
Cash and cash equivalents	$	5,562,158
Trade receivables		56,604
Inventories		46,575
Due from other governmental entities		1,460,501
Other current assets		304
Total current assets		7,126,142
Noncurrent assets		
Capital assets		61,481,532
Accumulated depreciation		(22,717,467)
Total noncurrent assets		38,764,065
Deferred outflows:		
Total deferred outflows		-
Total assets and deferred outflows		45,890,207
LIABILITIES		
Current liabilities		
Accounts payable		1,078,123
Accrued expenses		40,337
Compensated absences		51,551
Due to other governmental entities		530,730
Unearned revenue		3,364
Total current liabilities		1,704,105
Noncurrent liabilities		
Other post employment benefit liability		474,590
Unearned revenue		66,571
Total noncurrent liabilities		541,161
Total liabilities		2,245,266
Deferred inflows:		
Total deferred inflows		-
Total liabilities and deferred inflows		2,245,266
NET POSITION		
Invested in capital assets, net of related debt		38,764,065
Unrestricted		4,880,876
Total net position	$	43,644,941

The Accompanying Notes Are An Integral Part Of These Financial Statements

WEST VIRGINIA STATE RAIL AUTHORITY
STATEMENT OF REVENUES, EXPENSES, AND CHANGES IN NET POSITION
YEAR ENDED JUNE 30, 2013

Operating revenues		
Freight	$	2,269,323
Miscellaneous		208,542
Total operating revenues		2,477,865
Depreciation expense		1,773,843
Other operating expenses		3,590,324
Total operating expenses		5,364,167
Operating income (loss)		(2,886,302)
Nonoperating revenues (expenses)		
Intergovernmental revenue		3,200,765
Interest income		20,966
Grant revenue		558,802
Gain (loss) on disposition of assets		(68,411)
Total nonoperating revenues (expenses)		3,712,122
Change in net position		825,820
Total net position - beginning		42,819,121
Total net position - ending	$	43,644,941

The Accompanying Notes Are An Integral Part Of These Financial Statements

WEST VIRGINIA STATE RAIL AUTHORITY
STATEMENT OF CASH FLOWS
YEAR ENDED JUNE 30, 2013

Cash flows from operating activities	
Cash received from customers and government	$ 2,459,872
Cash paid to employees	(672,683)
Cash paid to suppliers and government	(1,408,385)
Net cash provided (used) by operating activities	378,804
Cash flows from noncapital financing activities	
Transfers in from State of West Virginia	1,974,246
Net cash provided (used) by noncapital financing activities	1,974,246
Cash flows from capital and related financing activities	
Federal railroad assistance	360,752
Purchase of capital assets	(3,117,830)
Net cash provided (used) by capital and related financing activities	(2,757,078)
Cash flows from investing activities	
Receipts of interest	20,966
Net cash provided (used) by investing activities	20,966
Increase (decrease) in cash and cash equivalents	(383,062)
Cash and cash equivalents, beginning of year	5,945,220
Cash and cash equivalents, end of year	$ 5,562,158
Reconciliation of operating income to net cash provided (used) by operating activities	
Operating loss	(2,886,302)
Adjustments to reconcile operating income to net cash provided (used) by operating activities	
Depreciation	1,773,843
Changes in operating assets and liabilities	
(Increase) decrease in trade receivables	(14,629)
(Increase) decrease in inventories	(14,045)
(Increase) decrease in other current assets	1,888
Increase (decrease) in accounts payable	999,837
Increase (decrease) in accrued expenses	(3,822)
Increase (decrease) in compensated absences	(1,532)
Increase (decrease) in due to other governmental entities	519,187
Increase (decrease) in unearned revenue	(3,364)
Increase (decrease) in OPEB	7,743
Net cash provided (used) by operating activities	$ 378,804

NOTE 1 - DESCRIPTION OF ORGANIZATION AND FINANCIAL REPORTING ENTITY

In 1975, the West Virginia Legislature created the West Virginia State Rail Authority (the Authority) under the provisions of Chapter 29, Article 18 of the Code of West Virginia, 1931, as amended, known as the "West Virginia Railroad Maintenance Act." The Authority was created to participate in the rehabilitation, improvement, and restoration of the financial stability of the railway system in the State of West Virginia and enable it to remain viable in the public sector as a mode of transportation. The Authority maintains the South Branch Valley Railroad and the West Virginia Central Railroad, and is responsible for the rails-to-trails program operation. The Secretary of Transportation serves as a member of the Authority, and the remaining six members are appointed by the Governor.

In evaluating how to define the Authority for financial reporting purposes, management has considered all potential component units. The decision to include a potential component unit in the reporting entity is made by applying the criteria set forth in accounting principles generally accepted in the United States of America. Accounting principles generally accepted in the United States of America define component units as those entities which are legally separate governmental organizations for which the appointed members of the Authority are financially accountable, or other organizations for which the nature and significance of their relationship with the Authority are such that exclusion would cause the Authority's financial statements to be misleading. Since no such organizations exist which meet the above criteria, the Authority has no component units. The Authority is an enterprise fund and a component unit of the West Virginia Department of Transportation and the State of West Virginia. Accordingly, the Authority's financial statements are discretely presented in the financial statements of the State of West Virginia.

NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

Basis of Accounting - The Authority is considered an enterprise fund and uses the flow of economic resources measurement focus and the accrual method of accounting. Under this method, revenues are recorded when earned and expenses are recorded when incurred. Enterprise funds are operated in a manner similar to private business enterprises where the intent of the governing body is that the cost (expense, including depreciation) of providing goods and services to the general public on a continuing basis be financed or recovered primarily through user charges.

NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (Continued)

Financial Statement Presentation - The Authority prepares its financial statements in accordance with GASB Statement No. 34, *Basic Financial Statements and Management Discussion and Analysis - for States and Local Governments*, as amended.

Use of Estimates - The preparation of financial statements in conformity with accounting principles generally accepted in the United States of America requires management to make certain estimates and assumptions that affect the amounts reported in the financial statements and accompanying notes. Actual results could differ from management's estimates.

Cash and Cash Equivalents - For purposes of the statement of net position, the Authority considers all highly liquid investments with an original maturity of three months or less to be cash equivalents.

Cash and cash equivalents balances on deposit with the State of West Virginia Treasurer's Office (the "State Treasurer") are pooled by the State Treasurer with other available funds of the State for investment purposes by the West Virginia Board of Treasury Investments (BTI). These funds are transferred to the BTI, and the BTI is directed by the State Treasurer to invest the funds in specific external investment pools in accordance with West Virginia Code, policies set by the BTI, provisions of bond indentures, and the trust agreements when applicable. Balances in the investment pools are recorded at fair value or amortized cost, which approximates fair value. Fair value is determined by a third-party pricing service based on asset portfolio pricing models and other sources, in accordance with GASB Statement No. 31, *Accounting and Financial Reporting for Certain Investments and for External Investment Pools.* The BTI was established by the State Legislature and is subject to oversight by the State Legislature. Changes in fair value and investment income are allocated to participants in the pools based upon the funds that have been invested. The amounts on deposit are available for immediate withdrawal on the first day of each month for the WV Short Term Bond Pool and, accordingly, are presented as cash and cash equivalents in the accompanying financial statements.

The BTI maintains the Consolidated Fund investment fund, which consists of investment pools and participant-directed accounts, in three of which the Authority may invest. These pools have been structured as multi-participant variable net asset funds to reduce risk and offer investment liquidity diversification to the Fund participants. Funds not required to meet immediate disbursement needs are invested for longer periods. A more detailed discussion of the BTI's investment operations pool can be found in its annual report. A copy of that annual report can be obtained from the following address: 1900 Kanawha Blvd. East, Room E-122, Charleston, West Virginia 25305 or http://www.wvbti.com.

NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (Continued)

Permissible investments for all agencies include those guaranteed by the United States of America, its agencies and instrumentalities (U.S. Government obligations); corporate debt obligations, including commercial paper, which meet certain ratings; certain money market funds; repurchase agreements; reverse repurchase agreements; asset-backed securities; certificates of deposit; state and local government securities (SLGS); and other investments. Other investments consist primarily of investments in accordance with the Linked Deposit Program, a program using financial institutions in West Virginia to obtain certificates of deposit, loans approved by the legislature and any other program investments authorized by the legislature.

Allowance for Doubtful Accounts - It is the Authority's policy to provide for future losses on uncollectible accounts, contracts, grants, and loans receivable based on an evaluation of the underlying account, contract, grant, and loan balances, the historical collectability experienced by the Authority on such balances, and such other factors which, in the Authority's judgment, require consideration in estimating doubtful accounts.

Inventories - Inventories are stated at the lower of cost or market; cost is valued using the weighted average cost method.

Capital Assets - Purchases of capital assets are capitalized at cost and, except for land, which is not depreciated, are depreciated using the straight-line method over the estimated useful lives of the assets ranging from five to forty years. Buildings, railroad infrastructure and land with an initial cost of $25,000 or more and furniture and equipment with an initial cost of $5,000 or more are recorded at cost. When assets are disposed of, the cost and related accumulated depreciation are removed from the accounts and any resulting gain or loss is recognized in operations. The cost of maintenance and repairs is charged to operations as incurred; significant renewals and betterments are capitalized. Capital assets are reviewed annually for impairment.

Compensated Absences and Other Post-Employment Benefits - Employees fully vest in all earned but unused annual leave, and the Authority accrues for obligations that may arise in connection with compensated absences for vacation at the current rate of employee pay. Effective July 1, 2007, the Authority adopted GASB Statement No. 45, *Accounting and Financial Reporting by Employers for Postemployment Benefits Other than Pensions*. This statement provided standards for the measurement, recognition, and display of other postemployment benefit (OPEB) expenditures, assets, and liabilities, including applicable note disclosures and required supplementary information.

NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (Continued)

During fiscal year 2006, House Bill No. 4654 was established to create a trust fund for postemployment benefits for the State of West Virginia (the "State"). Effective July 1, 2007, the Authority was required to participate in this multiple employer cost-sharing plan, the West Virginia Retiree Health Benefit Trust Fund, sponsored by the State of West Virginia. Details regarding this plan can be obtained by contacting Public Employees Insurance Agency ("PEIA"), 601 57th Street, SE, Suite 2, Charleston, WV 25304-2345 or http://www.wvpeia.com.

The Authority's full-time employees earn up to two vacation leave days for each month of service and are entitled to compensation for accumulated, unpaid vacation leave upon termination. Full-time employees also earn one and one-half sick leave days for each month of service and are entitled to extend their health insurance coverage upon retirement in lieu of accumulated, unpaid sick leave. Generally, two days of accrued sick leave extend health insurance for one month of single coverage and three days extend health insurance for one month of family coverage. For employees hired after 1988, the employee shares in the cost of the extended benefit coverage to the extent of 50% of the premium required for the extended coverage. Employees hired July 1, 2001 or later are not eligible for these benefits. During 2010, the legislature passed a bill allowing regular full-time employees hired before July 1, 2001, having accumulated at least 65 days of sick leave, to be paid, at their option, for a portion of their unused sick leave, not to exceed the number of sick leave days that would reduce the employee's sick leave balance to less than fifty days. The employee shall be paid at a rate equal to one quarter of their usual rate of daily pay during that calendar year. The liability for postemployment health care benefits is now provided for under the multiple employer cost-sharing plan sponsored by the State of West Virginia.

Deferred Inflows/Outflows - A deferred inflow of resources is an acquisition of net position that is applicable to a future reporting period. A deferred outflow of resources is a consumption of net position that is applicable to a future reporting period. The Authority accounts for deferred inflows and outflows of resources in accordance with the provisions of GASB Statement No. 63, *Financial Reporting of Deferred Outflows of Resources, Deferred Inflows of Resources, and Net Position* and GASB Statement No. 65, *Items Previously Reported as Assets and Liabilities.* The Authority did not have any deferred inflows/outflows of resources at June 30, 2013.

Operating Revenues and Expenses - Balances classified as operating revenues and expenses are those which comprise the Authority's ongoing operations. Principal operating revenues are charges to customers for use of the rail lines. Principal operating expenses are the costs of providing the goods and services and include administrative expenses and depreciation of capital assets. Other revenues and expenses are classified as non-operating in the financial statements.

NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (Continued)

Net Position - As required by GASB 34, the Authority displays net position in three components, if applicable: invested in capital assets, net of related debt; restricted; and unrestricted.

Investment in Capital Assets, Net of Related Debt - This component of net position consists primarily of capital assets, including restricted capital assets (if any), net of accumulated depreciation and reduced by the outstanding balances of any bonds, mortgages, notes or other borrowings that are attributable to the acquisition, construction, or improvement of those assets.

Restricted Net Position - Restricted net position represents the assets whose use or availability has been restricted, and the restrictions limit the Authority's ability to use the resources to pay current liabilities. When both restricted and unrestricted resources are available for use, it is the Authority's policy to use restricted resources first, then unrestricted resources as needed. As of June 30, 2013, there was no restricted net position.

Unrestricted Net Position - Unrestricted net position consists of net position that does not meet the definition of "restricted" or "invested in capital assets, net of related debt." In the governmental environment, net position is often designated to indicate that management does not consider it to be available for general operations. These types of constraints on resources are internal and management can remove or modify them. Such internal designations are not reported on the face of the statement of net position.

Transfers - Transfers represent legally authorized appropriations under West Virginia State Code by the West Virginia Legislature.

Newly Adopted Statements Issued By GASB

The Governmental Accounting Standards Board has also issued Statement No. 63, *Financial Reporting of Deferred Outflows of Resources, Deferred Inflows of Resources, and Net Position – an amendment of GASB Statements No. 3, No. 6, No. 10, No. 15, No. 17, No. 23, No. 25, No. 27, No. 28, No. 31, and No. 33*, effective for fiscal years beginning after December 15, 2011. This statement provides financial reporting guidance for deferred outflows of resources and deferred inflows of resources. The adoption of GASB Statement No. 63 had no financial impact on the June 30, 2013 financial statements it only improved readability.

NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (Continued)

The Governmental Accounting Standards Board has also issued Statement No. 65, *Items Previously Reported as Assets and Liabilities*, effective for fiscal years beginning after December 15, 2012. This statement will improve financial reporting by clarifying the appropriate use of the financial statement elements deferred outflows of resources and deferred inflows of resources to ensure consistency in financial reporting. The early adoption of this statement had no financial impact on the June 30, 2013 financial statements it only improved readability.

The Governmental Accounting Standards Board has also issued Statement No. 66, *Technical Corrections-2012-an amendment of GASB Statements No. 10 and No. 62*, effective for fiscal years beginning after December 15, 2012. This statement will resolve conflicting accounting and financial reporting guidance that could diminish the consistency of financial reporting and thereby enhance the usefulness of the financial reports. The adoption of this Statement did not have a material effect on the financial statements.

Recent Statements Issued By GASB

The Governmental Accounting Standards Board has also issued Statement No. 67, *Financial Reporting for Pension Plans-an amendment of GASB Statement No. 25*, effective for fiscal years beginning after June 15, 2013. This statement will improve financial reporting primarily through enhanced note disclosures and schedules of required supplementary information that will be presented by the pension plans that are within its scope. The Authority has not yet determined the effect that the adoption of GASB Statement No. 67 may have on its financial statements.

The Governmental Accounting Standards Board has also issued Statement No. 68, *Accounting and Financial Reporting for Pensions-an amendment of GASB Statement No. 27*, effective for fiscal years beginning after June 15, 2014. this Statement will improve the decision-usefulness of information in employer and governmental nonemployer contributing entity financial reports and will enhance its value for assessing accountability and interperiod equity by requiring recognition of the entire net pension liability and a more comprehensive measure of pension expense. The Authority has not yet determined the effect that the adoption of GASB Statement No. 68 may have on its financial statements

The Governmental Accounting Standards Board has also issued Statement No. 69, *Government Combinations and Disposals of Government Operations*, effective for fiscal years beginning after December 15, 2013. This statement establishes accounting and financial reporting standards related to government combinations and disposals of government operations. The Authority has not yet determined the effect that the adoption of GASB Statement No. 69 may have on its financial statements.

NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (Continued)

The Governmental Accounting Standards Board has also issued Statement No. 70, *Accounting and Financial Reporting for Nonexchange Financial Guarantees*, effective for fiscal years beginning after June 15, 2013. This Statement will improve the accounting and financial reporting by state and local governments that extend and receive nonexchange financial guarantees. The Authority has not yet determined the effect that the adoption of GASB Statement No. 70 may have on its financial statements.

NOTE 3 - CASH AND CASH EQUIVALENTS

The composition of cash and cash equivalents were as follows at June 30, 2013:

	Amortized Cost	Estimated Fair Value
Cash on deposit with State Treasurer	$ 55,500	$ 55,500
Cash on deposit with State Treasurer invested in BTI (WV Money Market Pool)	3,468,113	3,468,113
Cash on deposit with State Treasurer invested in BTI (WV Short Term Bond Pool)	2,038,545	2,038,545
	$ 5,562,158	$ 5,562,158

BTI DISCLOSURE INFORMATION

The BTI has adopted an investment policy in accordance with the "Uniform Prudent Investor Act." The "prudent investor rule" guides those with responsibility for investing the money for others. Such fiduciaries must act as a prudent person would be expected to act, with discretion and intelligence, to seek reasonable income, preserve capital, and, in general, avoid speculative investments. The BTI's investment policy is to invest assets in a manner that strives for maximum safety, provides adequate liquidity to meet all operating requirements, and achieves the highest possible investment return consistent with the primary objectives of safety and liquidity. The BTI recognizes that risk, volatility, and the possibility of loss in purchasing power are present to some degree in all types of investments. Due to the short-term nature of the Consolidated Fund, the BTI believes that it is imperative to review and adjust the investment policy in reaction to interest rate market fluctuations/trends on a regular basis and has adopted a formal review schedule. Investment policies have been established for each investment pool and account of the Consolidated Fund of the BTI's Consolidated Fund pools and accounts in which the Authority invest, all are subject to credit risk.

NOTE 3 - CASH INVESTMENTS AND CASH EQUIVALENTS (Continued)

WV Money Market Pool - Credit Risk

Credit risk is the risk that an issuer or other counterparty to an investment will not fulfill its obligations. For the year ended June 30, 2013, the WV Money Market Pool, has been rated AAAm by Standard & Poor's. A fund rated "AAAm" has extremely strong capacity to maintain principal stability and to limit exposure to principal losses due to credit, market, and/or liquidity risks. "AAAm" is the highest principal stability fund rating assigned by Standard & Poor's. Neither the BTI itself nor any of the other Consolidated Fund pools or accounts has been rated for credit risk by any organization. The WV Money Market Pool is subject to credit risk.

The BTI limits the exposure to credit risk in the WV Money Market Pool by requiring all corporate bonds to be rated AA- by Standard & Poor's (or its equivalent) or higher. Commercial paper must be rated at least A-1 by Standard & Poor's and P-1 by Moody's. The pool must have at least 15% of its assets in U.S. Treasury issues. At June 30, 2013, the WV Money Market Pool investment had a total carrying value of $2,495,868,000 of which the Authority's ownership represents .14%.

WV Short Term Bond Pool - Credit Risk

The BTI limits the exposure to credit risk in the WV Short Term Bond Pool by requiring all corporate bonds to be rated A by Standards & Poor's (or its equivalent) or higher. Commercial paper must be rated at least A-1 by Standards & Poor's and P-1 by Moody's. Mortgage-backed and asset-backed securities must be rated AAA by Standard & Poor's and Aaa by Moody's. As this pool has not been rated, the following table provides information on the credit ratings of the WV Short Term Bond Pool's investments (in thousands):

NOTE 3 - CASH INVESTMENTS AND CASH EQUIVALENTS (Continued)

		Credit Rating			
Security Type		Moody's	S&P	Carrying Value	Percent of Pool Assets
Corporate asset backed securities		Aaa	AAA	$ 53,681	8.72%
		Aaa	NR	59,810	9.71
		NR	AAA	37,411	6.07
		NR	AA+	2,514	0.41
	*	Caa1	CCC	932	0.15
	*	Caa3	D	367	0.06
	*	Caa3	NR	24	0.00
	*	Ca	CCC	308	0.05
	*	Ca	D	95	0.02
	*	NR	NR	3,819	0.62
Corporate bonds and notes		Aa2	AA+	3,002	0.49
		Aa2	AA	12,731	2.07
		Aa2	AA-	9,192	1.49
		Aa3	AA-	33,034	5.36
		Aa3	A+	11,693	1.90
		A1	AA+	13,295	2.16
		A1	AA	4,118	0.67
		A1	A+	47,500	7.71
		A1	A	13,522	2.19
		A2	A+	9,348	1.52
		A2	A	47,709	7.75
		A2	A-	5,052	0.82
		A3	A-	7,986	1.30
	*	Baa1	A-	2,416	0.39
	*	Baa2	A-	6,959	1.13
U.S. agency bonds		Aaa	AA+	9,986	1.62
U.S. Treasury notes **		Aaa	AA+	140,154	22.76
U.S. agency mortgage backed securities ***		Aaa	AA+	73,692	11.97
Money market funds		Aaa	AAAm	5,457	0.89
				$ 615,807	100.00%

NR = Not Rated

* These securities were not in compliance with BTI Investment Policy at June 30, 2013. The securities were in compliance when originally acquired, but were subsequently downgraded. BTI management and its investment advisors have determined that it is in the best interests of the participants to hold the securities for optimal outcome.

** U.S. Treasury issues are explicitly guaranteed by the United States government and are not subject to credit risk.

*** U.S. agency mortgage backed securities are explicitly guaranteed by the United States government and are not subject to credit risk.

At June 30, 2013, the Authority's ownership represents 0.33% of these amounts held by the BTI.

Interest Rate Risk

Interest rate risk is the risk that changes in interest rates will adversely affect the fair value of an investment. All Consolidated Fund pools and accounts are subject to interest rate risk.

NOTE 3 - CASH INVESTMENTS AND CASH EQUIVALENTS (Continued)

The overall weighted average maturity of the investments of the WV Money Market Pool cannot exceed 60 days. Maximum maturity of individual securities cannot exceed 397 days from date of purchase, except for government floating rate notes, which can be up to 762 days. The following table provides information on the weighted average maturities for the various asset types in the WV Money Market Pool:

Security Type	2013 Carrying Value (In Thousands)	WAM (Days)
Repurchase agreements	$ 229,326	3
U.S. Treasury notes	279,755	132
U.S. Treasury bills	34,993	77
Commercial paper	970,395	43
Certificates of deposit	259,000	66
U.S. agency discount notes	445,784	47
Corporate bonds and notes	10,000	60
U.S. agency bonds	66,603	139
Money market funds	200,012	1
	$ 2,495,868	52

The overall effective duration of the investments of the WV Short Term Bond Pool cannot exceed 731 days. Maximum effective duration of individual securities cannot exceed 1,827 days (five years) from date of purchase. The following table provides information on the effective duration for the various asset types in the WV Short Term Bond Pool:

Security Type	Carrying Value (In Thousands)	Effective Duration (Days)
U.S. Treasury notes	$ 140,154	491
Corporate bonds and notes	227,557	293
Corporate asset backed securities	158,961	471
U.S. agency bonds	9,986	583
U.S. agency mortgage backed securities	73,692	60
Money market funds	5,457	1
	$ 615,807	358

Other Risks of Investing

Other risks of investing can include concentration of credit risk, custodial credit risk, and foreign currency risk. None of the Consolidated Fund's investment pools or accounts is exposed to these risks as described below.

Concentration of credit risk is the risk of loss attributed to the magnitude of a Consolidated Fund pool or account's investment in a single corporate issuer. The BTI investment policy prohibits those pools and accounts permitted to hold corporate securities from investing more than 5% of their assets in any one corporate name or one corporate issue.

NOTE 3 - CASH INVESTMENTS AND CASH EQUIVALENTS (Continued)

The custodial credit risk for investments is the risk that, in the event of the failure of the counterparty to a transaction, the BTI will not be able to recover the value of investment or collateral securities that are in the possession of an outside party. Repurchase agreements are required to be collateralized by at least 102% of their value, and the collateral is held in the name of the BTI. The BTI or its agent does not release cash or securities until the counterparty delivers its side of the transaction.

Foreign currency risk is the risk that changes in exchange rates will adversely affect the fair value of an investment or a deposit. None of the Consolidated Fund's investment pools or accounts holds interests in foreign currency or interests valued in foreign currency.

Deposits

Custodial credit risk of deposits is the risk that in the event of failure of a depository financial institution, a government will not be able to recover deposits or will not be able to recover collateral securities that are in the possession of an outside party. Deposits include nonnegotiable certificates of deposit. None of the above pools contain nonnegotiable certificates of deposit. The BTI does not have a deposit policy for custodial credit risk.

NOTE 4 - CAPITAL ASSETS

Capital assets balances and the activity for the year ended June 30, 2013 is summarized below:

	June 30, 2012 Balance	Additions	Deletions	June 30, 2013 Balance
Capital assets				
Land	$ 4,835,588	$ 457,500	$ -	$ 5,293,088
Land improvements	228,957	-	-	228,957
Buildings and improvements	554,060	-	-	554,060
Office equipment	45,325	-	-	45,325
Work equipment	1,935,640	190,642	-	2,126,282
Locomotives, freight and passenger cars	2,995,311	34,819	-	3,030,130
Railroad infrastructure	47,893,275	2,434,869	124,454	50,203,690
Total capital assets	$ 58,488,156	$ 3,117,830	$ 124,454	$ 61,481,532
Accumulated depreciation				
Land improvements	$ 97,195	$ 16,489	$ -	$ 113,684
Buildings and improvements	348,824	13,646	-	362,470
Office equipment	45,271	-	-	45,271
Work equipment	1,174,530	98,797	-	1,273,327
Locomotives, freight and passenger cars	1,319,329	127,728	-	1,447,057
Railroad infrastructure	18,014,518	1,517,183	56,043	19,475,658
Total accumulated depreciation	$ 20,999,667	$ 1,773,843	$ 56,043	$ 22,717,467

NOTE 5 - RELATED PARTY TRANSACTIONS WITH THE STATE OF WEST VIRGINIA

The Authority enters into certain transactions with various agencies of the State of West Virginia. The following summarizes the nature and terms of the most significant transactions.

The Authority's employees participate in various benefit plans offered by the State of West Virginia. Employer contributions to these plans are mandatory. During the year ended June 30, 2013, the Authority incurred payroll related expenditures of approximately $90 thousand for employee health insurance benefits provided through the West Virginia Public Employees Insurance Agency and approximately $67 thousand in employer matching contributions to the State Public Retirement System. The Authority also paid the West Virginia Department of Highways approximately $1.5 million for bridge replacement, engineering services, labor and materials. In addition, during the year ended June 30, 2013, the Authority received transfers of $3,200,765 in appropriated funds. A significant decrease in this revenue or assistance would have a significant effect on the operations of the Authority.

At June 30, 2013, the Authority had amounts due from the State of West Virginia of $1,262,451. The Office of the Secretary of Administration, Finance Division transferred $1,938,314 to the Authority for the year ended June 30, 2013.

NOTE 6 - SIGNIFICANT CUSTOMERS AND FUNDING SOURCES

During the year ended June 30, 2013, approximately 87.2% of the Authority's freight traffic was attributable to a single customer.

The credit and liquidity crisis in the United States and throughout the global financial system triggered significant events and substantial volatility in world financial markets and the banking system that have had a significant negative impact on foreign and domestic financial markets. If the aforementioned single customer is affected, it could have a significant impact on the future operations of the Authority.

NOTE 7 - RISK MANAGEMENT

The Authority is exposed to various risks of loss related to torts; theft of, damage to, and destruction of assets; errors and omissions; injuries to employees; employee health and life coverage; and natural disasters. The State of West Virginia established the Board of Risk and Insurance Management (BRIM) and the Public Employees Insurance Agency (PEIA) public entity risk pools to account for and finance uninsured risks of losses for state agencies, institutions of higher education, and component units.

BRIM is a public entity risk pool that provides coverage for general, liability, and property damage in the amount of $1,000,000 per occurrence. Such coverage may be provided to the Authority by BRIM through self-insurance programs maintained by BRIM or policies underwritten by BRIM that may involve experience-related premiums or adjustments to BRIM. BRIM engages an independent actuary to assist in the determination of its premiums so as to minimize the likelihood of premium adjustments to the Authority or other participants in BRIM's insurance program. As a result, management does not expect significant differences between the premiums the Authority is currently charged by BRIM and the ultimate cost of that insurance based on the Authority's actual loss experience. Furthermore, there have been no settlements that have exceeded this coverage in the last three years.

Through its participation in the PEIA, the Authority has obtained health, life, and prescription drug coverage for all its employees. The Authority, through a third-party insurer has obtained coverage for job-related injuries for its employees. In exchange for payment of premiums to PEIA and a third-party insurer, the Authority has transferred its risks related to health, life, prescription drug coverage, and job-related injuries. PEIA issues publicly available financial reports that include financial statements and required supplementary information; these reports may be obtained by writing to West Virginia Public Employees Insurance Agency, 601 57th Street, Charleston, WV 25304 or by calling 1-888-680-7342.

American Zurich Insurance Company provides workers' compensation coverage to all West Virginia state agencies. Payments for coverage are made directly to the West Virginia State Insurance Commission who in turn purchases the workers' compensation coverage on behalf of all West Virginia state agencies. Nearly every employer in the state who has a payroll must have coverage.

In exchange for premiums, the Authority transfers its risk of loss related to employee injuries to American Zurich Insurance Company.

NOTE 8 - OTHER POSTEMPLOYMENT BENEFITS

Plan Description - The Authority participates in the West Virginia Other Postemployment Benefits Plan (OPEB Plan) of the West Virginia Retiree Health Benefit Trust Fund, a cost-sharing multiple-employer defined benefit postemployment healthcare plan administered by the West Virginia Public Employees Insurance Agency (WVPEIA). The OPEB Plan provides retiree postemployment healthcare benefits for participating state and local government employers. The provisions of the Code of West Virginia, 1931, as amended (the "Code"), assigns the authority to establish and amend benefit provisions to the WVPEIA Board of Trustees. The WVPEIA issues a publicly available financial report that includes financial statements and required supplementary information for the OPEB Plan. That report may be obtained by writing to Public Employees Insurance Agency, 601 57th Street, SE, Suite 2, Charleston, WV 25301-2345 or by calling 1-888-680-7342.

Funding Policy - The Code requires the OPEB Plan bill the participating employers 100% of the annual required contributions (ARC), an amount actuarially-determined in accordance with the parameters of GASB Statement No. 45. The ARC represents a level of funding that, if paid on an ongoing basis, is projected to cover normal cost each year and amortize any unfunded actuarial liabilities (or funding excess) of the plan over a period not to exceed thirty years. State of West Virginia plan employers are billed per active health policy per month.

The Authority's ARC was $38,893, $154,113, and $183,191 and the Authority has paid premiums of $31,150, $27,753, and $36,786, which represent 80.1%, 18.0%, and 20.1% of the ARC, respectively, for the years ended June 30, 2013, 2012, and 2011. At June 30, 2013, the liability related to OPEB costs was $474,590.

The West Virginia Legislature passed legislation to provide alternate funding sources for the RHBT OPEB unfunded liability. In addition, the PEIA Finance Board imposed limits on the retiree subsidy currently provided for PEIA premiums for retirees. Future increases in the subsidy will be limited to no more than 3% per year. These actions have had a material impact on the amounts billed by the RHBT to the Authority in the current year as well as an expected material impact on amounts billed in the future, resulting in decreases in the recorded OPEB liability.

NOTE 9 - RETIREMENT PLAN

PLAN DESCRIPTION - The Authority contributes to the West Virginia Public Employees Retirement System (PERS), a cost-sharing multiple-employer defined benefit pension plan administered by the West Virginia Consolidated Public Retirement Board. Chapter 5, Article 10 of the West Virginia State Code assigns the authority to establish and amend benefits provisions to the PERS Board of Trustees. Employees who retire at or after age 60 with five or more years of contributory service or who retire at or after age 55 and have completed 25 years of credited service are eligible for retirement benefits as established by State statute. Retirement benefits are payable monthly for life, in the form of a straight-line annuity equal to two percent of the employee's final average salary multiplied by the number of years of the employee's credited service at the time of retirement. PERS also provides deferred retirement, early retirement, death, and disability benefits to plan members and beneficiaries. The West Virginia Consolidated Public Retirement Board issues a publicly available financial report that includes financial statements and required supplementary information for PERS. That report may be obtained by writing to the West Virginia Consolidated Public Retirement Board, 4101 MacCorkle Avenue, SE, Charleston, WV 25304-1636 or by calling (304) 558-3570.

Funding Policy - The PERS funding policy has been established by action of the State Legislature. State statute requires that plan participants contribute 4.5% of compensation. The current combined contribution rate is 18.5% of annual covered payroll, including the Authority's contribution of 14.0%, which is established by PERS. Effective July 1, 2013, an increase in the contribution rate of .5%, will increase the Authority's contribution rate to 14.5%. The Authority's contributions to PERS for the years ended June 30, 2013, 2012, and 2011 were $67,408, $71,450 and $64,099, respectively.

NOTE 10 - COMMITMENTS AND CONTINGENCIES

Periodic Audits

Under the terms of federal grants, periodic audits are required and certain costs may be questioned as not being appropriate expenditures under the terms of the grants. Such audits could lead to reimbursement to the grantor agencies. The Authority management believes disallowances, if any, will not have a significant financial impact on the Authority's financial position.

Litigation

Periodically, there are various claims and legal proceedings against the Authority arising from the normal course of business. Currently, there are no pending claims or legal proceedings against the Authority.

ADDITIONAL INFORMATION

Suttle & Stalnaker PLLC
CERTIFIED PUBLIC ACCOUNTANTS

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH *GOVERNMENT AUDITING STANDARDS*

To the Members
West Virginia State Rail Authority
Moorefield, West Virginia

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the financial statements of the business-type activities of the West Virginia State Rail Authority (the Authority) as of and for the year ended June 30, 2013, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements, and have issued our report thereon dated October 22, 2013.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Authority's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses, or, significant deficiencies. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Authority's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards.*

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. The report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Suttle & Stalnaker, PLLC

Charleston, West Virginia
October 22, 2013

Service Organization Control 1 Report

Description of West Virginia Office of Technology Data Center Services

For the period July 1, 2012 through June 30, 2013

with Independent Service Auditor's Report
including Tests Performed and Results Thereof

West Virginia Office of Technology

Data Center Services

TABLE OF CONTENTS

Report of Management on West Virginia Office of Technology's Data Center Services

STATE OF WEST VIRGINIA
DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY
State Capitol
Charleston, West Virginia 25305

Earl Ray Tomblin
Governor

Ross Taylor
Cabinet Secretary

Gale Y. Given
Chief Technology Officer

West Virginia Office of Technology's Management Assertion

October 11, 2013

We have prepared the accompanying West Virginia Office of Technology (WVOT) data center services, including the general controls over the West Virginia Financial Information Management System (WVFIMS), (Description) for users of the system during some or all of the period July 1, 2012 to June 30, 2013 (user entities), and the independent auditors of user entities who have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. The Company confirms, to the best of its knowledge and belief, that:

a. The Description fairly presents the data center services, including the general controls over WVFIMS, (System) made available to user entities during the period July 1, 2012 to June 30, 2013 for data center services. The criteria we used in making this assertion were that the Description:

(1) Presents how the System made available to user entities was designed and implemented, including

- The types of services provided.
- The procedures, within both automated and manual systems, by which those services are provided to user entities.
- The related supporting information; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities.
- How the System captures and addresses significant events and conditions.
- The process used to prepare reports or other information provided to user entities.
- Specified control objectives and controls designed to achieve those objectives.
- Controls that, in designing the System, the Company contemplated would be implemented by user entities in order to achieve the specified control objectives (Complementary User Entity Controls).
- Other aspects of the Company's control environment, risk assessment process, information and communication systems (including the related business

processes), control activities, and monitoring controls that are relevant to the services provided.

(2) Does not omit or distort information relevant to the scope of the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and the independent auditors of user entities, and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in the user entity's own particular environment.

b. The Description includes relevant details of changes to the System during the period from July 1, 2012 to June 30, 2013.

c. The controls related to the control objectives stated in the Description, which together with the complementary user entity controls referred to above if suitably designed and operating effectively, were suitably designed and operated effectively throughout the period July 1, 2012 to June 30, 2013 to achieve those control objectives. The criteria we used in making this assertion were that

(1) The risks that threaten the achievement of the control objectives stated in the Description have been identified by the service organization.

(2) The controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

(3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Independent Service Auditor's Report

Building a better
working world

Ernst & Young LLP
2100 One PPG Place
Pittsburgh, PA 19522

Tel: +1 412 644 7800
Fax: +1 412 644 0477
ey.com

Independent Service Auditor's Report

To the Management of West Virginia Office of Technology

Scope

We have examined West Virginia Office of Technology's (WVOT) accompanying *Description of Data Center Services*, including general controls over the West Virginia Financial Information Management System (WVFIMS), throughout the period July 1, 2012 to June 30, 2013 (Description) and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description. The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of WVOT's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information in the accompanying *Other Information Provided by WVOT* is presented by management of WVOT to provide additional information and is not part of WVOT's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

WVOT's responsibilities

WVOT has provided the accompanying assertion titled, *Report of Management on WVOT's Data Center Services* (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description. WVOT is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls to achieve the related control objectives stated in the Description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls described therein are suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period July 1, 2012 to June 30, 2013.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls described therein to achieve the related control objectives stated in the Description involves performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives, and the suitability of the criteria specified by the service organization and described in the Assertion. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their independent auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in WVOT's Assertion:

a. the Description fairly presents the *WVOT's Data Center Services* that was designed and implemented throughout the period July 1, 2012 to June 30, 2013.

b. the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2012 to June 30, 2013 and if user entities applied the complementary user entity controls contemplated in the design of WVOT's controls throughout the period July 1, 2012 to June 30, 2013.

c. the controls tested, which, together with the complementary user entity controls referred to in the scope paragraph of this report if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved and operated effectively throughout the period July 1, 2012 to June 30, 2013.

Description of tests *of controls*

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying *Description of Control Objectives, Controls, Tests and Results of Tests* (Description of Tests and Results).

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of WVOT, user entities of *WVOT's Data Center Services* during some or all of the period July 1, 2012 to June 30, 2013, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Ernst + Young LLP

October 11, 2013
Pittsburgh, PA

Description of West Virginia Office of Technology Data Center Services

for the period July 1, 2012 through June 30, 2013

Overview of the West Virginia Office of Technology Organization

The State of West Virginia – West Virginia Office of Technology (WVOT) was established in June 2005 to consolidate Information Technology (IT) infrastructure, develop an organized approach to IT resource management, and provide technical assistance to agencies. Through the planning process, the WVOT evaluates the economic justification, suitability for purpose, the current and future technology environment, regulatory requirements and other factors to make recommendations on the purchase, lease or acquisition of IT resources. Additionally, the WVOT evaluates and approves contracts for acquisition of IT products and services by the State spending units. The WVOT, under the Department of Administration (DOA), and its Chief Technology Officer (CTO) with respect to Executive agencies will:

- Develop a unified and integrated structure for information systems for all Executive agencies;
- Establish, based on need and opportunity, priorities and time lines for addressing the information technology requirements of the various Executive agencies of State government;
- Overrule and supersede decisions made by the administrators of the various Executive agencies of government with respect to the design and management of information systems and the purchase, lease or acquisition of information equipment and contracts for related service;
- Draw upon staff of other Executive agencies for advice and assistance in the formulation; and implementation of administrative and operational plans and policies; and
- Recommend to the Governor transfers of equipment and human resources from any Executive agency and the most effective and efficient uses of the fiscal resources of Executive agencies, to consolidate or centralize information-processing operations.

The CTO and directors have the necessary expertise in IT, experience in the design and management of information systems and an understanding of the special demands upon government with respect to budgetary constraints, the protection of privacy interests and federal and state standards of accountability to assist agencies in meeting the needs of their constituents.

The WVOT has currently established Memorandums of Understanding (MOU) and Service Level Agreements (SLA) with Core Consolidated Customers, which are defined as members of those agencies that have consolidated under the Office of Technology. In addition, the WVOT provides over 30 fee-based technology services and products to Core Consolidated Customers, as well as other State agencies. The service rates are established in accordance with federal cost allocation guidelines as noted in the Office of Management and Budget Circular A-87.

Description of the Control Environment, Information and Communication, Monitoring and Risk Assessment Processes

The WVOT's control environment represents the overall attitude, awareness, and actions of the administration of the Executive Branch, and others concerning the importance of controls, and the appropriate emphasis given to controls in the WVOT's policies, procedures, practices, and organizational structure. The following is a description of the components of the WVOT's system of internal control.

Control Environment

Management Philosophy

The DOA's mission is to operate a cost-efficient, customer-oriented service department whose actions are transparent to taxpayers resulting in innovative solutions and quality results for a government that effectively serves West Virginians.

The WVOT's goals are to develop an organized approach to information technology resource management for the State, while providing technical assistance to State entities in the design and management of information systems. Through the planning process, the WVOT will evaluate, in conjunction with the Information Services and Communications unit, the economic justification, system design and suitability of information technology resources equipment and related services, and review and make recommendations on the purchase, lease, or acquisition of information technology equipment and contracts for related services by the State spending units.

The WVOT strives for continuous improvement through the establishment of the following strategic goals:

- Maintain the highest levels of customer satisfaction.
- Make government services more accessible.
- Implement common infrastructure and business applications.
- Ensure State information assets are secured and privacy is protected.
- Lower costs and improve the quality of the State's technical infrastructure.
- Strengthen our technology workforce.

Additionally, the WVOT Office of Information Security and Controls (OISC) has established an information security strategic plan to identify the key elements of the West Virginia Executive Branch Information Security Program and provide direction for the implementation and maintenance of controls to protect the State's data and technology resources. The current strategic plan, finalized and adopted in 2010, encompasses the following information security initiatives:

- Security policy development
- Privacy partnership
- Risk management
- Business continuity plans
- Disaster recovery plans

- Security Operations Center (SOC) and security operations
- Training and culture
- Information security management emphasis
- IT audit program
- Certification and accreditation (for technology products and services)
- Incident management and computer forensics
- Funding
- Team development
- Information security metrics
- Outreach
- Office of Technology partners
- West Virginia information security principles

Commitment to Integrity

The WVOT is committed to maintaining the highest possible standards of ethical business conduct. Its officers and employees are expected to be free of any influence, interest or relationship that might conflict with the best interests of the State. This includes maintaining a workplace free from the effects of drug and alcohol abuse.

According to the West Virginia Ethics Act, full-time public servants may not take personal regulatory action on matters affecting a person (1) by whom they are secondarily employed or (2) with whom they are seeking employment or have an agreement concerning future employment.

The West Virginia Ethics Act also prohibits full-time public servants from seeking or accepting employment from persons or businesses that they or their subordinates regulate. The Act prohibits full-time public servants from seeking or accepting employment from vendors if the public servant, or his or her subordinates, exercise authority or control over a public contract with that vendor. It does not apply to members of the Legislature.

The West Virginia Division of Personnel's Secondary Employment Policy explains that State service shall be the primary employment of every employee. Any secondary employment/volunteer activity must not: interfere with, conflict with, or have the appearance of a conflict with an employee's primary State employment; conflict with the interests of the State agency; interfere with the performance of the employee's official duties; use proprietary State information; create the appearance of official State action; or entail appearing before the State agency for which he or she is employed on behalf of the secondary employer or volunteer organization in any capacity.

As directed by the West Virginia Department of Personnel's Drug and Alcohol Policy: it is the policy of West Virginia State government to ensure that its workplaces are free of alcohol, illegal drugs and controlled substances by prohibiting the use, possession, purchase, distribution, sale, or having such substances in the body system. Although the sale and use of alcohol by an adult may be legal, the possession, use, distribution, or dispensation of alcohol in the workplace is strictly prohibited.

The State of WV Equal Employment Opportunity Office (EEO) was created to establish an equal Employment Opportunity Program for all State agencies and State employees. The State EEO promotes the belief that all West Virginians have the right to equal employment opportunities regardless of race, religion, color, national origin, ancestry, sex, age, disability, or other legally-recognized protected status. It is the goal of the State EEO to assist State agencies in a joint effort to maintain a workplace free of discrimination and to ensure equal employment opportunities for everyone. The State of West Virginia is firmly committed to this policy and ensuring its adherence is the principal mission of the State EEO.

WVOT Employee Core Values

The WVOT exists to support State agencies, other government entities and citizens in realizing objectives through technology. Specifically, the WVOT will:

- Have a passion for work and the success of customers and clients.
- Pursue change and continuous improvement with a sense of urgency.
- Earn the respect of customers by consistently delivering as promised.
- Hold ourselves accountable for everything we do.
- Leverage proven technologies and management methods in defining, designing and delivering quality business solutions.
- Be responsive to customer needs based on their view of business impact.
- Work as a team and respect co-workers and peers.

Segregation of Duties

The WVOT is structurally organized to support the internal control of segregation of duties by separating the duties authorization, custody, record keeping and reconciliation with respect to transaction processing, application development and maintenance, technology operations and database management. Segregation of duties within the WVOT is governed by:

- Access to data and technology resources is limited based on an individual's job responsibility.
- Access to data and technology is governed by the minimum information necessary rule, which limits data access to the "minimum necessary to accomplish the intended purpose."
- Requests for access to infrastructure resources (e.g., mainframe, network, and shared drives) are processed by the WVOT Account Management Unit.
- Designated Approval Authorities (DAA) must authorize all requests for access to and use of infrastructure resources.
- Reconciliation of transaction processing jobs is the responsibility of individuals who submitted the job or their designee.

The WVOT Account and Configuration Management Unit

The WVOT has an account management unit that is responsible for the establishment of a single user ID per State employee and user provisioning – the creation, change and removal of user accounts from the network, establishment and management of user home directories, network shares, network printing assignments, network group management, and VPN accounts.

Designated Approval Authorities

A designated approval authority is a supervisor, manager, or director who authorizes access to resources and assumes responsibility for ensuring that the access is appropriate for job duties, and issuing a request to terminate access when no longer needed. The WVOT account management team requires that a DAA signs network login forms and shared resource access forms before permitting access.

Controls Related to Personnel Management

The West Virginia Division of Personnel (DOP) was created by statute in 1989 to provide leadership in human resource management for the executive operating agencies of State government, including administration of a merit system (i.e., civil service). A comprehensive system of personnel management is achieved through the integration of six functional areas:

- Classification and Compensation Section
- Employee Communications Section
- Employee Information/Payroll Audit Section
- Employee Relations Section
- Organization and Human Resource Section Development
- Staffing Services Section

The WVOT adheres to the WV DOP Administrative Rules, which govern classification plans, pay plans, open competitive examinations, promotions, layoff and recall, appointments, dismissals, demotions, and other human resource matters consistent with the West Virginia Code. The WVOT also follows DOP Policies, which provide directives for Work Place Security, Supervisory Training, Providing, and Obtaining Employment References, and New Employee Hiring Process.

Position Descriptions

Written job descriptions have been established to formally delineate employee job responsibilities. The values and behavior standards of WVOT are communicated to all personnel through policy statements and formal codes of conduct. Each job description issued by Personnel has the following set of criteria:

- Nature of work – summary of position
- Distinguishing characteristics – any characteristics that distinguish the duty from other positions (e.g., supervisory position, level of impact on enterprise and/or departmental operations, etc.)
- Essential job functions – specific job duties
- Knowledge, skills, and abilities – any additional skills or abilities, which will enhance understanding of the position
- Minimum qualifications – training, education, experience, and substitutions for both

WVOT New Employee (New Hire) Procedures

When a State job is posted, all applicants must go through the same new hire process, as directed by the State Division of Personnel. WVOT has developed formal policies and procedures available on the internal SharePoint site.

Prior to hiring within the WVOT, a "new hiring restriction" memo from the CTO to the department secretary is prepared for approval. This memo justifies why the position should be filled. The questions range from why the position is needed, to alternatives to filling the position, to the consequences of leaving the position vacant. A memo is not required in all instances given the job posting process under justification.

All prospective employees must complete the appropriate paperwork (e.g., tax forms, employee ID, parking forms, etc.). All prospective employees must also have a background check prior to employment. All new hire paperwork is collected on an employee's first day and it is verified using a check list that all forms have been received.

Employee Performance Appraisals (EPA)

The WVOT utilizes performance appraisals to identify, measure, and evaluate an employee's job-related behaviors and accomplishments during a specific period of time and compares those to previously established performance standards. The EPA system is characterized by clearly-defined performance goals and objectives and increased employee involvement.

The WVOT follows the Division of Personnel's Employee Performance Appraisal Policy, DOP-17. This document states that the State of West Virginia must:

- Advise employees what is expected of them during the first 30 days of each performance rating period (which shall not exceed 12 consecutive months in length).
- Provide feedback to employees regarding how well they are doing near the midpoint of the performance rating period.
- Formally rate employees at the end of each performance rating period.

Risk Management

WVOT's risk assessment process identifies and manages risks that could affect its ability to provide reliable IT services and solutions to its clients. WVOT identifies significant risks based on:

- Financial and/or operational value and impact
- Legal and/or regulatory requirements
- Input provided by the WVOT Internal IT Audit group based on audit findings
- Input provided by the service auditor based on the service auditor's examination

The specific approach for IT risk assessment is outlined in the OISC Information Security Strategic Plan. This plan describes risk as the relationship between *value, threats, and vulnerabilities*. In the absence of any value, threat, or vulnerability, no risk exists. Value of data tends to increase in most State organizations, and since the complete elimination of threats and/or vulnerabilities is impossible, some risk will always exist. The reduction of externally based threats is generally not possible, although many threats can be blocked if they are known. Focus and resources must therefore be directed primarily at the reduction of vulnerabilities.

The WVOT follows an ongoing, cyclic approach to risk management: Risk Assessment, Risk Mitigation and Evaluation and Re-Assessment. This approach includes the following initiatives:

Initiative 1: Review system characterizations: purpose, scope, criticality, platform, complexity, etc.

Initiative 2: Identify existing threats and vulnerabilities

Initiative 3: Analyze existing controls to determine actual use and effectiveness

Initiative 4: Determine likelihood and impact

Initiative 5: Create a risk matrix to separate those risks that are unacceptable from those that are tolerable

Initiative 6: Conduct a cost-benefit analysis to determine how well, or how poorly, a planned action will turn out and whether the planned action is advisable

Initiative 7: Determine a risk mitigation strategy based upon cost-benefit analysis

Initiative 8: Recommend changes in controls/countermeasures

Initiative 9: Complete mitigation activities

Initiative 10: Monitor system for changes and repeat process at appropriate intervals

Monitoring

Monitoring for potential failures in internal controls is a combination of having a robust organization structure, and a series of defined activities where WVOT interfaces with its customers. Currently, the WVOT OISC provides monitoring services in the form of an internal IT audit program and through the Security Operations Center (SOC).

The WVOT maintains and manages an objective, internally independent information security audit program. This program serves the Executive Branch by examining, evaluating, and reporting on information technology applications, systems, operations, processes, and practices to provide reasonable assurance that security controls will:

- Safeguard information assets and protect privacy;
- Preserve the integrity and reliability of data;
- Function as intended to achieve the entity's objectives; and
- Comply with standards, policies, and regulations.

Audit efforts are focused on those operational areas presenting the highest degree of risk, as well as the greatest potential for benefit to the Executive Branch. Internal Audit recommendations are designed to help Executive Branch agencies reduce risk, and establish and sustain effective internal controls. Executive Branch agencies are mandated to submit or undergo periodic audits to confirm compliance with mandated security requirements. External auditors have the right to audit the State agency or make other provisions to ensure that the State agency is maintaining adequate safeguards.

The WVOT SOC monitors all consolidated agencies that terminate into the WVOT managed network. A brief description of the monitoring tools is provided below:

- A monitoring tool that collects security events from a heterogeneous set of sources that includes network infrastructure, security devices, servers, and applications. It normalizes all events to enable automatic out-of-the-box correlation with other events and network flows. In addition, it surveys the entire network, using native flow sources in a customer's routing/switching infrastructure or data from distributed collectors to gather a detailed history of all network flow activity.
- An intrusion detection tool capable of stopping attacks at the perimeter of the threat and proactively protecting against future threats and vulnerabilities. This tool offers an extensive range of detection capabilities, as well as host-based and network-based deployment options.
- An Internet content filtering tool provides web-based filtering for all consolidated agencies. This tool facilitates safe and productive use of the Internet by filtering and/or blocking access to specific websites.

Information and Communication

Management is closely involved in both the strategic and operational aspects of WVOT's business. Management encourages frequent staff meetings and open communication at all levels. WVOT has implemented a number of communication methods to assist all employees in understanding their roles and responsibilities, and to help confirm that significant events are communicated to an appropriate level of management in a timely manner. These methods include formal security and privacy training for new employees and the use of online policies and procedures.

The CTO and the directors strive to maintain positive relationships with WVOT employees and Executive agencies. All WVOT employees are encouraged to attend annual staff meetings, which are used as a time to announce new IT policies, to introduce new control functions and internal control procedures, for new software demonstrations, and to evaluate customer satisfaction and employee performance levels, etc. During annual staff meetings, field staff is rotated so that regions are covered as well as the service desk. This ensures that customer service is ongoing even though majority of WVOT employees are attending the staff meetings.

The WVOT Project Steering Committee holds periodic meetings to approve and prioritize projects involving the WVOT. This Committee is composed of the WVOT CTO and directors, managers and members of the Project Management Office. In addition to approving and prioritizing projects, this Committee monitors project status (schedule, scope and budget) confirms resource assignments and addresses issues that cannot be resolved at the project team level.

The WVOT holds weekly Operations meetings to discuss operational activities scheduled for the upcoming week and address any issues that have developed during the past week. Additionally, the various unit managers provide updates about upcoming assignments and operational activities.

WVOT has also implemented a number of communication methods to assist employees in understanding their roles and responsibilities, and to help confirm that significant events are communicated to an appropriate level of management in a timely manner. SharePoint is utilized to relay information to employees within WVOT. Information included on the SharePoint site consists of: the latest news and events, training opportunities, personnel news/updates, tools, operations updates, WVOT job postings, etc. Other methods include using the Learning Management System tool for formal security training, and the use of e-mail to distribute security and privacy tips, instances of system maintenance or anti-virus updates, new IT policy announcements, and e-mails pertaining to Executive agencies to members of the Governor's Executive Information Security Team (GEIST). Additionally, informal methods of communication such as Facebook and Twitter are utilized to provide information such as job postings.

The Governor's Executive Information Security Team (GEIST)

Security-related information affecting Executive Branch agencies are also e-mailed to members of the GEIST. These individuals will in turn share the information with their respective Cabinet Secretaries and other appropriate individuals.

The GEIST is mandated by the Governor's Executive Order 6-06, and is led by the Office of Information Security and Controls (OISC). It comprises representatives who have been appointed by Cabinet Secretaries from all Executive Branch department-level organizations, with appropriate staff support, management, and leadership roles.

The mission of the GEIST is to reduce overall security related risk to State IT systems, and all data, through the development and communication of appropriate procedures, processes, and controls, with an emphasis on administrative controls. The GEIST supports an elevated understanding of the business critical data and systems, data classification, cultural change, audits, business continuity, and user awareness of individual and collective responsibilities in the protection of information confidentiality, integrity, and availability.

GEIST membership consists of Executive Branch agency information security administrators (ISA), who have been appointed by their respective Cabinet Secretaries. These individuals must maintain frequent contact with their Cabinet Secretaries, and possess institutional knowledge of their agency. Membership will also include OISC representation, as appropriate.

Responsibilities of GEIST members include, but are not limited to, facilitating: (1) development of information security policy, training in that policy, auditing for policy compliance, and assuring the effective remediation of findings of deficiencies or non-compliance with that policy; (2) completing an IT-related risk analysis of agency systems, rating systems by business criticality, and documenting threats and vulnerabilities; (3) overseeing the classification of agency systems, including both electronic and non-electronic forms of data; and (4) overseeing the completion of mandatory information security training for all agency employees.

WVOT Customer Relationship Managers

Customer relationship managers (CRM) are an agency's advocate within the WVOT, to ensure technical requirements are met and prioritized within the WVOT. An agency's CRM is an advocate who will maintain a positive relationship and be knowledgeable of political and business drivers. An agency will also be able to provide feedback to WVOT via the CRM to obtain existing State-approved technical solutions. A CRM acts as a business liaison for moving technology forward for an agency.

A CRM will keep the agency informed on all major software upgrades that will impact computing needs. When an agency identifies its technical needs, the CRM will help that agency take their functional business need, and provide technical options. All CRMs will actively work with their assigned agencies for the best technical solutions. Key objectives in fulfilling customer requirements are communication, technical needs analysis, and customer service.

Training / ELearning / State Learning Management System

The Technology Learning Center (TLC) is a unit within the WVOT, that:

- Offers instructor led and online classes for various PC-supported software packages used within State government.
- Assists agencies in the development, procurement assistance, or training on software for internal use in creating ELearning content.
- Manages the State Learning Management System for delivery and scheduling of learning content.
- Trains and assists agency personnel in managing their course content and using the State Learning Management System.

The TLC serves as the central resource for all State agencies in utilizing the best of technology to deliver effective learning opportunities to the State workforce.

TLC's training program has been developed for general State government activities, and because classes are small (only ten students), individual instruction is emphasized.

Classes are offered in a variety of formats: instructor-led hands-on training, instructor-led internet classroom using online collaboration software, and e-learning self-paced classes. Classes are designed to meet each individual's needs, whether he/she is a new or advanced user.

Additional areas of training include the Division of Personnel that recommends all individuals occupying supervisory, managerial and director level positions adhere to DOP Supervisor/Manager Training Program Policy, which states that, in addition to meeting the minimum requirements of the positions into which they have been placed, all supervisors and managers in associated agencies should successfully complete the Supervisor/Manager Training Program established by DOP policy.

Policies Issued by the CTO

Under the authority granted by the State Legislature in West Virginia Code (http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=05a&art=6#06), the CTO has the authority to direct the formulation and promulgation of policies, guidelines, standards and specifications for the development and maintenance of IT and technical infrastructure.

The WVOT has developed Executive Branch security standards, policies, and procedures for use by Executive organizations, and has provided best practices guidelines for all other State and local public sector organizations. With these policies as a framework, procedures portray specifically how the policies are implemented. Policies developed by Executive Branch agencies that address IT or information security issues may be more, but not less, stringent than those issued by the CTO.

A list of current WVOT polices includes the following:

- Information Security Policy
- Acceptable Use of Portable Devices
- Acceptable Use of State-Provided Instant Messaging
- Acceptable Use of State-Provided Wireless Devices
- Contractor Management
    - Contractor Information Form
    - Employment Confirmation
- Data Backup and Retention
- Data Classification
- E-mail Use Standards
- IT Policy and Procedure Development
- Information Security Audit Program
- Removable Media
- Use of Social Media
- Anti-Virus
- Accreditation and Certification
- Bar Coding
- Internet Usage
- Network Violation Reporting
- Wireless Access Points

A list of current WVOT procedures includes the following:

- Establishing and Implementing IT Policies and Procedures
- Requesting Technical Investigations
- End of Life Disk Drive Handling
- Account Management
- Domain Administrator Access
- WVOT Software Updates
- Information Security Audit Program
- Network Violation Management

Confidentiality Agreement

The WVOT created a revised version of the West Virginia Department of Administration Employee Confidentiality Agreement on July 1, 2009 and revised September 20, 2010. Employees must sign this document annually. This Agreement explains the importance of protected health information (PHI), personally identifiable information (PII), agency and State policies, and other confidential information and data systems.

Each employee who signs the Agreement must agree to use any special access to information only when absolutely necessary to administer the system(s) for which he/she is responsible and to refrain from obtaining or attempting to obtain confidential information for any unauthorized persons or uses. When that individual no longer has access to these records, he/she is bound by the document and must continue to maintain the confidentiality of information to which he/she previously had access.

(Source: WVOT Employee Confidentiality Agreement as of September 20, 2010.)

The WVOT Information Security policy (WVOT-PO1001), established on January 18, 2007 and revised November 10, 2009, outlines responsibilities for Executive Branch employees regarding confidentiality.

- The agency head must assure that all employees sign a confidentiality agreement upon hire and annually thereafter.
- Confidential, private, personally identifiable information (PII) or sensitive data (i.e., credit card numbers, calling card numbers, logon passwords, health information, or other protected information), must be encrypted or disassociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.
- If at any time equipment or media changes ownership or is ready for disposal, the user must alert the responsible technical staff to the potential presence of any confidential and/or sensitive data on said equipment or media.

Control Activities

Several control activities as implemented by the WVOT are described below.

The OISC Internal IT Audit Program

The WVOT maintains and manages an objective and internally independent internal audit program. Internal Audit serves the Executive Branch by examining, evaluating, and reporting on IT applications, systems, operations, processes, and practices to provide reasonable assurance that security controls will:

- Safeguard information assets and protect privacy;
- Preserve the integrity and reliability of data;
- Function as intended to achieve the entity's objectives; and
- Comply with standards, policies, and regulations.

Executive Branch agencies are mandated to submit to or undergo audits on a periodic basis to confirm compliance with mandated security requirements. External auditors have the right to audit the State agency or make other provisions to ensure that the State agency is maintaining adequate safeguards.

All WVOT IT auditors are bound by confidentiality standards, and are required to sign the Department of Administration Confidentiality Statement annually, as well as sign and abide by WVOT-PO1001, WVOT's Information Security policy.

The WVOT internal audit program will only release engagement findings and recommendations to additional entities under the following circumstances: by request from the audit client, for peer review, and/or under order of subpoena. Only information specific to the request will be released.

Audit efforts are focused on those areas and activities presenting the highest degree of risk, as well as the greatest potential for benefit to the Executive Branch. Internal Audit recommendations are designed to help Executive Branch agencies manage operations more securely. Types of audits include, but are not limited to: (1) account management, (2) application controls, (3) desktop practices, (4) disaster recovery, (5) network controls, (6) server management, (7) policy and regulatory compliance, and (8) technology acquisitions.

The WVOT provides three different information security audit services: a client self-assessment, a WVOT-performed audit, and a WVOT coordinated and managed examination performed by a third-party.

Generally, an information security audit involves five phases. These include (1) initiation and planning, (2) fieldwork (examination phase), (3) analysis and review, (4) final reporting, and (5) follow-up. Upon completion of the audit engagement, the client will receive a formal presentation and a report on the state of information security controls. This report includes findings as well as recommendations to correct or strengthen controls. After a reasonable period, Internal Audit will conduct a follow-up meeting to discuss any needed corrective or strengthening measures. The client can follow recommendations issued after a self-assessment to strengthen basic controls and perform advanced preparation for more in-depth audits or reviews.

The WVOT information security audit program has developed the rolling three-year security audit plan to select and schedule audits. This plan will be reviewed and revised annually by the Chief Information Security Officer (CISO) to ensure that current, significant risks are considered when selecting audit targets and may be modified at any time to meet the needs of the Executive Branch.

Project Management

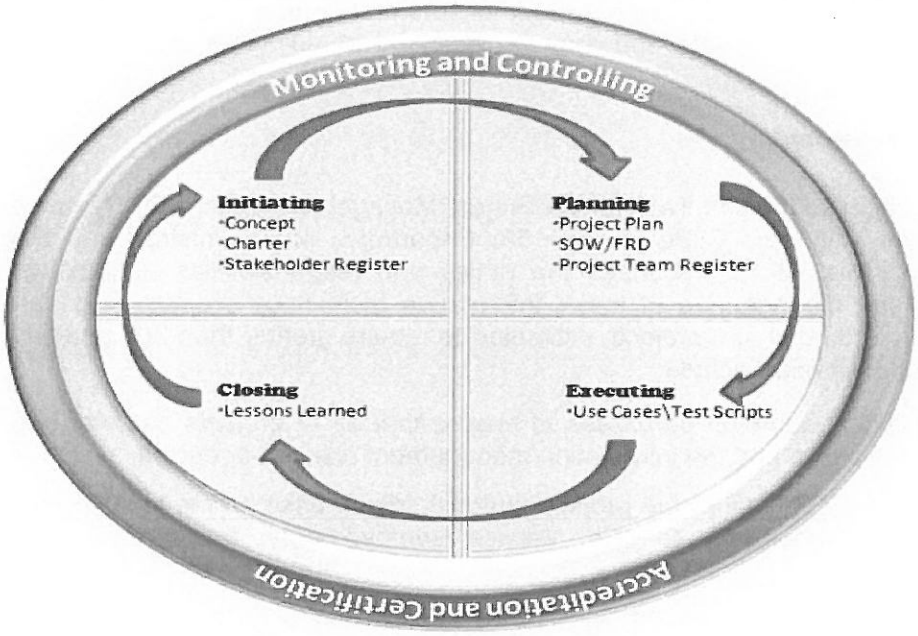
The West Virginia Office of Technology Project Management Office (PMO) was established in 2006 through WV State Code Chapter 5A. Department of Administration, Article 6 Office of Technology. This article prescribes the duties and responsibilities attributable to the CTO concerning the management of major information technology projects (e.g., projects valued greater than $100,000 and projects estimated to require greater than 300 person hours). Some specific responsibilities include:

- Implement approval processes to ensure that all IT projects conform to the Statewide strategic plan and the information management plans of agencies.
- Define and communicate project approval criteria base on the technical feasibility of the project, opportunity to offer service improvements, and ensure compliance with regulations.
- Provide project oversight services to ensure that projects achieve charter objectives according to the proposed schedule, budget and other key performance indicators.
- Develop a methodology for managing IT projects throughout the entire project life cycle and provide training on application of the methodology.
- Provide support and leadership across State government by establishing and enforcing standards for IT projects and training of agency project managers.
- Establish information project steering committees to provide ongoing direction for major information technology project and have the authority to approve or reject any changes to the project's scope, schedule or budget.

The WVOT PMO methodology follows a project management methodology that aligns with Project Management Body of Knowledge (PMBOK), which includes the following five processes:

1. **Initiating** is the process of defining a new project or a new phase of an existing project.
2. **Planning** is the process of establishing the scope, define objectives, gather requirements and define the actions to be taken to complete the project.
3. **Executing** is the process of completing the tasks defined during planning to meet the objects of the project.
4. **Monitoring and Controlling** is the process of tracking, reviewing, and regulating the progress of the project. One must also identify changes to the plan and initiate a change control process.
5. **Closing** is the process to finalize all tasks while obtaining certification of accuracy and accreditation of approval.

Overview of the WVOT Project Management Life Cycle



The Office of Information Security and Controls

The OISC was formed in 2007, and is charged with enhancing the overall information security posture of the Executive Branch of the West Virginia State Government. The goal is to reduce the overall risk to the data and the information systems that contain and process this data. Supporting Privacy Regulations are an important component of the Information Security mission.

To guide OISC's efforts, the focus is on three different requirements for data and systems:

- Confidentiality: Exposing data only to those with a need and right to use.
- Integrity: Keeping data values accurate, and altered only by an authorized person.
- Availability: Maintaining systems and communications to acceptable operational status.

To maintain confidentiality, integrity, and availability of data and systems, several types of controls are utilized:

- Technical (e.g., firewalls, intrusion detection/prevention, anti-virus, NAC, etc.)
- Administrative (e.g., policy, training, executive leadership, auditing, etc.)
- Physical (e.g., ID badges, door locks, security guards, surveillance cameras, etc.)

This enterprise approach to information security enables WV State Government to move forward in a coordinated and effective progression toward reduced risk. The concept of "layered security" involves the use of controls and protections at every opportunity in the information system landscape. Some of the layers in an effective information security program include: policies, technical controls (firewalls, access control lists in network equipment, anti-virus, spam filtering, website blocking, encryption, event monitoring, vulnerability scanning, configuration and patch management, etc.), awareness training leading to cultural change in the user community (locking unattended workstations, protecting passwords, handling and conveying sensitive information with regard to its content, etc.), management emphasis on risk reduction, minimum required privileges and access, segregation of duties, auditing for policy and regulatory compliance, and adequate physical security policy compliance. The WVOT has adopted the *ISO Information Security Standards* as the basis for defining the West Virginia information security objectives.

Organizational units within the WVOT work closely together, and particularly closely with Information Security, to ensure that the WVOT is creating and using standards in naming conventions, configurations, settings, documentation, and process creation and implementation. All of WVOT's initiatives and projects should have security objectives embedded within the architecture, and incorporated into the setup routine for all system components.

Each organization with a role in the technical setup and administration of system components should align their operational activities with the following fundamental security concepts:

- Least privilege – No assignment of privilege to anyone without a need for access
- Segregation of duties – Separation of responsibilities to ensure no conflict of interest, and to ensure accountability
- Documentation of security activities – Diligence is not verifiable without documentation
- Cross training to provide redundant skills in critical functional areas – Eliminate skills vulnerabilities
- Documentation of all configurations and system setup procedures – In the event of a failure or "disaster," restore and recovery operations may need to be completed by someone other than the primary technician assigned to the system support function. Thorough documentation reduces dependence on single or specific individuals during critical situations.
- Job control (over personnel) – Techniques used to ensure that critical functions cannot be adversely impacted by a single individual. Can include mandatory paid time off, rotation of responsibilities and implementation of requirements for multiple individuals to perform key functions.

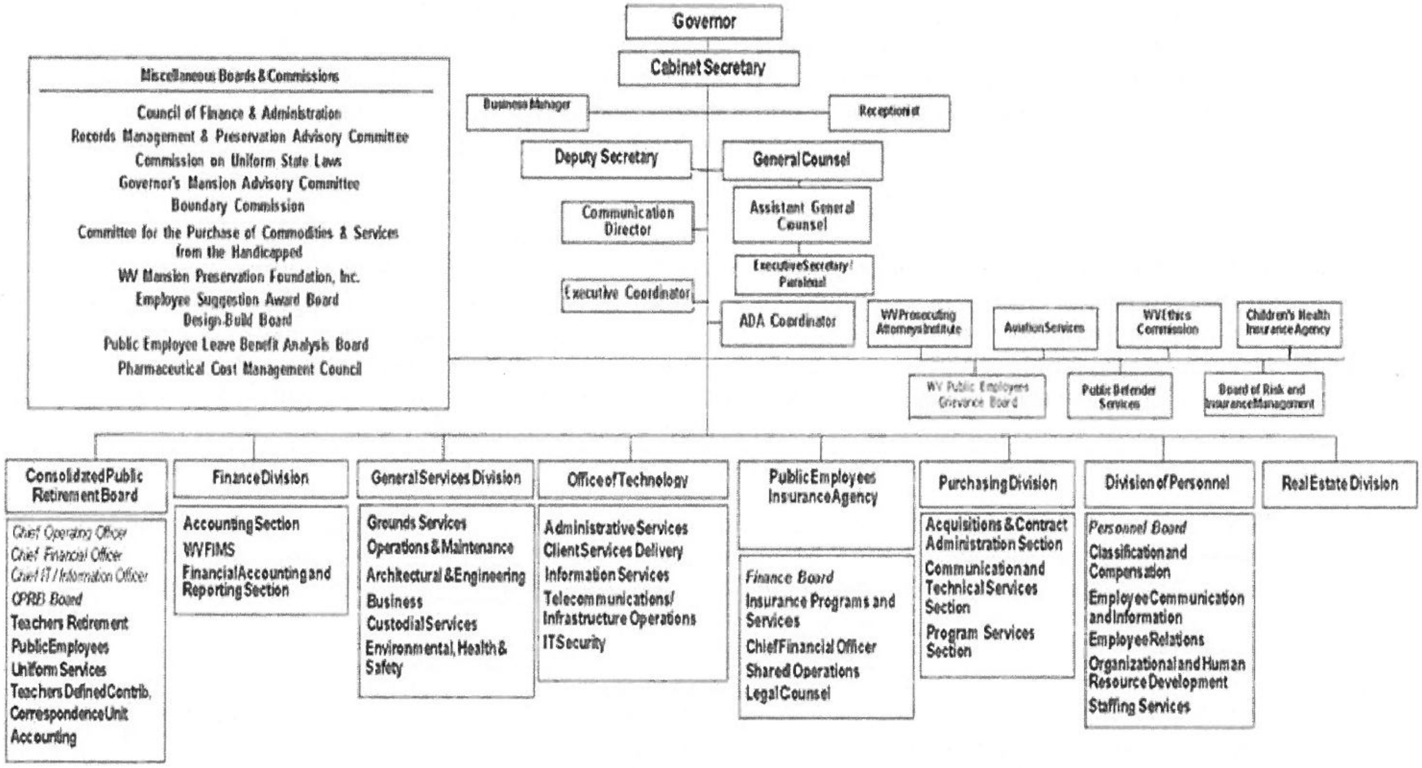
All State employees should understand the elements of their role in the protection of information systems and the data that these systems contain, and should also be responsible for their actions in the use of information systems, to support Information Security.

Organizational Structure and Assignment of Authority and Responsibility

The WVOT is organized into five departments consisting of more than 240 employees. The five departments are:

- **Administrative Services** – Provides accounting, asset management, contract management, IT purchasing, personnel management, technology billing, and time reporting functions.
- **Client Services Delivery** – Consists of several units providing technical support and assistance to other agencies. These units include the Service Desk, Field Support, Customer Relationship Management, Technology and Engineering of Health IT, Infrastructure Applications, and Technology Learning Center.
- **Information Services** – Offers software development and support, and database administration services. Also provides technology management services for WVFIMS – the State's financial system. Provides project management and provides consulting services for the acquisition of technology products and services.
- **Information Security and Controls** (OISC) – Provides the security operations center, information security awareness training, internal IT auditing services, and supports the CTO in the development, issuance and publication of IT policies and procedures.
- **Telecommunications and Infrastructure Operations** – Manages the WVOT data center, servers and storage, network operations, and telephony services. Also provides systems engineering services.

A West Virginia Department of Administration organization chart, which includes the WVOT, is presented below.


Governor
Cabinet Secretary
Business Manager
Receptionist
Deputy Secretary
General Counsel
Communication Director
Assistant General Counsel
Executive Secretary / Paralegal
Executive Coordinator
ADA Coordinator
Miscellaneous Boards & Commissions
Council of Finance & Administration
Records Management & Preservation Advisory Committee
Commission on Uniform State Laws
Governor's Mansion Advisory Committee
Boundary Commission
Committee for the Purchase of Commodities & Services from the Handicapped
WV Mansion Preservation Foundation, Inc.
Employee Suggestion Award Board
Design-Build Board
Public Employee Leave Benefit Analysis Board
Pharmaceutical Cost Management Council
WV Prosecuting Attorneys Institute
Aviation Services
WV Ethics Commission
Children's Health Insurance Agency
WV Public Employees Grievance Board
Public Defender Services
Board of Risk and Insurance Management
Consolidated Public Retirement Board
Chief Operating Officer
Chief Financial Officer
Chief IT / Information Officer
CPRB Board
Teachers Retirement
Public Employees
Uniform Services
Teachers Defined Contrib.
Correspondence Unit
Accounting
Finance Division
Accounting Section
WVFIMS
Financial Accounting and Reporting Section
General Services Division
Grounds Services
Operations & Maintenance
Architectural & Engineering
Business
Custodial Services
Environmental, Health & Safety
Office of Technology
Administrative Services
Client Services Delivery
Information Services
Telecommunications/ Infrastructure Operations
IT Security
Public Employees Insurance Agency
Finance Board
Insurance Programs and Services
Chief Financial Officer
Shared Operations
Legal Counsel
Purchasing Division
Acquisitions & Contract Administration Section
Communication and Technical Services Section
Program Services Section
Division of Personnel
Personnel Board
Classification and Compensation
Employee Communication and Information
Employee Relations
Organizational and Human Resource Development
Staffing Services
Real Estate Division

Services

The WVOT provides over 30 different technology products and services to the Core Consolidated Customers, as well as other State agencies. This section contains a description of some of those products and services. Of these services, those included in the *Description of Control Objectives, Controls, Tests, and Results of Tests* are as follows: Information Services Applications Development, Centralized Mainframe Data Storage and Recovery Services, Distributed Servers, Mainframe Computing, Network/Backbone Connectivity, Contact Center Services, User Account Management, and WVFIMS.

Information Services Applications Development (Programmer Analyst Services)

The Applications Development Center (ADC) of the WVOT is responsible for providing application software development and support to State agencies. The ADC is responsible for maintaining and supporting several key business applications, including the statewide Human Resource Information System (HRIS), the statewide Position Information Management System (PIMS), the statewide Leave System and full database support for the statewide West Virginia Financial Information Management System (WVFIMS).

Anti-virus

The WVOT provides anti-virus programs to the agencies for comprehensive protection against viruses and other malicious computer code known as “malware.” This protection includes the tools and procedures necessary to prevent major and widespread damage to user applications, files, desktops, laptops, and servers that are either physically or remotely connected to the State network via a standard network, wireless, modem, or through a virtual private network (VPN).

Centralized Mainframe Data Storage and Recovery Services

This service provides data storage and backup copies of data. Other components of this service include support and maintenance of hardware, systems software, and other infrastructure resources. Systems programming and disaster recovery services are provided as applicable.

Distributed Servers

The WVOT follows two models for server management: centralized server management and distributed server management. Servers owned by an individual agency, but managed by the WVOT are defined as distributed servers. Included in distributed service management are the following services:

- Proactive monitoring and maintenance of platform hardware, to include warranty repair as needed.
- Centrally administered patch management deployment for operating system and application support.
- Centrally administered antivirus software for each system.
- Backup monitoring and restoration.
- Operating system administration.
- Hardware specification for procurement to support life cycle management.

E-mail

The WVOT standard e-mail service is provided using Microsoft Outlook and Microsoft Exchange. Microsoft Outlook is a personal information manager providing e-mail, calendar, tasks, and contact management. Also, the standard e-mail service provides web access, spam and content filtering, a common address book, Office Communicator, and 24/7 support.

E-mail Encryption

E-mail encryption provides the agencies with the ability to send e-mails and attachments using the Advanced Encryption Standard (AES) encryption algorithm when transmitting e-mail and attachments outside the enterprise (State network).

Information Security Auditing (IT Auditing)

Information security audit services provide an objective, internally independent, examination of information security controls related to data, systems, operations, personnel, policies, processes, and practices. The WVOT internal IT audit program reports functionally and administratively to the Chief Information Security Officer (CISO).

Common audit areas include, but are not limited to:

- Account management
- Application controls
- Desktop practices
- Disaster recovery
- Network controls
- Server management
- Policy and regulatory compliance
- Technology acquisitions

The WVOT provides three different information security audit services: a client self-assessment, a WVOT-performed audit, and a WVOT coordinated and managed examination performed by a third-party. Generally, an information security audit involves five phases. Audits can last from a few days to several months, depending on the scope and objectives of the audit work. Internal IT audit recommendations are designed to help Executive Branch agencies manage operations more securely, resulting in a more appropriate use of resources.

Information Security Threat Management and Incident Response

The WVOT offers information security threat management and incident response services to assist agencies with safeguarding citizens' data. These services also assist the agencies in implementing an information security program, which will enable them to quickly react to real and potential cyber security incidents. The WVOT's overall goal is to help the agencies prepare for, protect against, detect, respond to, and recover from possible computer incidents. Agencies will benefit from these services because they offer an informed approach to threat management, as well as an increased understanding and awareness of information security vulnerabilities.

Services include:

- Threat assessment
- Coordination of governmental security operations throughout the State

- Security consulting
- Incident response

Investigative and Forensic Services

The WVOT provides computer forensic investigations for State agencies. These investigations utilize technical expertise and tools to meet agency investigative needs. The Office of Information Security and Controls (OISC) team includes experienced technical personnel who can assist agencies through the complex processes of managing e-discovery, employee computer/network misconduct, or cyber incidents related to service outage, compromise, or breach of data. Forensic Services offers customers:

- Industry standard forensic tools
- Forensically sound collection and analysis of evidence
- Identification of vulnerable systems/applications or misuse
- Containment of compromise
- Identification of policy violations
- Recommendations for repairing discovered vulnerabilities
- Post-repair device scanning and evaluation

Mainframe Computing (Day, Night, Teleprocessing, Priority)

The mainframe is an IBM z-Series enterprise server that supports a variety of State agency applications. The service includes transaction execution, equipment, systems software, maintenance of hardware and software, systems programming, disaster recovery services, and infrastructure.

Network/Backbone Connectivity

This service provides the local/wide area infrastructure, which is necessary for users to access and transmit data/voice/video throughout the State network with speed and innovation. It is designed to deliver the core data communications for most State and non-State entities who access State electronic resources. Users connect to a common, integrated platform that enables data movement between applications/systems/processes, and enhances the ability to communicate electronically both internally and externally from the State network.

PC Support

The WVOT provides a managed desktop service for agencies to meet service level agreements regarding personal computing requirements. Specifically, this service provides a consistent and reliable client computing environment to end user customers. Desktop Support is responsible for configuring each PC with standard software so that State employees have established standard computing programs available to them for performing their duties. The personal computers shall also be configured so the WVOT is able to access the individual machines for installation and support of software, distribution of patches, and for repairs and anti-virus scanning. Additionally, this service covers support of associated standard computing peripherals such as printers, scanners, PDAs, smart phones, and digital cameras.

Project Management

Project Management is the discipline of planning, organizing, and managing resources to bring about the successful completion of specific project goals and objectives. Clients should arrange for WVOT project management services when they want to follow a formal project management methodology to achieve project goals and objectives while controlling scope, quality of deliverables, schedule, and budget. The WVOT project management methodology includes the following processes: initiating, planning, executing, closing-out, and control/monitoring. The CTO has been charged with developing an approval process for proposed major information technology projects by State agencies to ensure that all projects conform to the statewide strategic plan and the information management plans of agencies. The Project Management Office, working with the CTO, will implement the approval and monitoring process for information technology projects. Accordingly, Project Management will lead, assist, or provide oversight (depending on level of services requested) for the development of project goals and objectives, schedules, resource allocation plans, backup and recovery plans, communication plans, executive reporting, risk management plans, identification and implementation of operational and security controls, certification and testing steps, accreditation and approval activities, issue tracking and resolution, budget monitoring, etc.

Telephony Support

The internet protocol telephony (IPT)/traditional voice and contact center services products include the equipment, network infrastructure, and services that enable employees to access/distribute voice communications from their desktop or the regional agency offices throughout the State network, i.e., the services required to deliver dial tone and contact center agents. Some specific telephony services include, but are not limited to:

IP Telephony/Traditional Voice Services

- Inventory: Telephony hardware/software, call recording hardware/software, desktop handsets, soft phone applications, voice mail hardware/software, and local voice circuits.
- Service provision: Purchase and support of hardware/software, troubleshooting, repair, administration, and engineering of the voice infrastructure to include standard/current versions of operating software. Additional activities include management, compliance reviews, service level management, Moves/Adds/Changes, and maintenance agreements.

Contact Center Services

- Inventory: Contact Center hardware/software, routing control services hardware/software, circuits (inbound and outbound calls), contact agents, and maintenance.
- Service provision: Purchase and support of hardware/software, troubleshooting and repair, administration and engineering of upgrades to the contact center infrastructure, maintenance, service level management, and compliance reviews.

Training

The IT training unit, led by certified Microsoft trainers, includes a variety of products and services:

- Instructor-led training is delivered in both the physical classroom setting and virtual classroom through the web. Courses include standard Microsoft desktop tools, specialized software products on demand, customized courses based on customer or agency need
- Self-paced, web-based training for Microsoft products

- Design and development of custom agency business training courses for delivery through the web
- Online registration and scheduling tools. Customers who are sponsoring conferences utilize this tool to register attendees and schedule them for individual conference sessions
- A learning management system (LMS) to deliver and track online training

The WVOT service catalog provides customers with a comprehensive listing of WVOT technology products, services and related rates, which includes additional information about training provisions.

User Account Management

User account management and directory services include establishment of a single user ID per State employee and user provisioning, i.e., the creation, change and removal of user accounts from the network, establishment and management of user home directories, network shares, network printing assignments, network group management, and VPN accounts. It is important from both a cost and security perspective, to ensure that accounts for employees who leave the organization are removed from the network. Compliance with the account management process for proper notification of employee transfer and termination will ensure that the agency is charged only for active employees, while preserving security.

Web Filtering

Web filtering is a service that constantly monitors all Internet site access requests by users, and blocks access for State employees to sites that are categorized as inappropriate or malicious. This monitoring is governed by Section 5.4.1.2 of the WVOT Information Security policy, which states: "The State reserves the right to filter Internet site availability and monitor employee use as required for legal, audit, or legitimate authorized State operational or management purposes." WVOT uses an Internet content filtering application to manage Internet access. This assists in ensuring that:

- Inappropriate or malicious content is not being viewed and/or downloaded from the Internet or distributed to fellow colleagues.
- Viruses, spyware, malware and other malicious applications do not degrade network performance or lead to data leakage of confidential information.
- Unauthorized use of application protocols, such as Instant Messaging and Peer-2-Peer file sharing, are not limiting network bandwidth or being abused to transfer sensitive data.

WVFIMS

The West Virginia Financial Information Management System (WVFIMS) is the State's accounting system. The WVOT supports the storage of the production and warehouse databases, backups of the production and warehouse databases, refreshes of the warehouse, programming support for problem fixes and enhancements, and interfaces with other systems.

Description of IT General Control Objectives

Application Software Development

WVOT has developed a change management process as it relates to the production WVFIMS application. Modifications are made based on the end-user needs and requirements of the business and client (agencies). WVOT has developed a formalized procedure outlining the application change management process from initiation through completion **(Control 1.1)**.

Initiation and authorization of changes

The programmers/analysts responsible for the maintenance and enhancement of the WVFIMS application receive requests for system changes from different types of users including:

- Users who use WVFIMS daily in the normal course of their work to add, modify, and inquire on transactions and accounts.
- Users from organizations who use WVFIMS to regulate, monitor, or control the finances of the State such as the State Auditor's Office (SAO), the State Treasurer's Office (STO), the State Budget Office, and the Purchasing and Finance divisions of the Department of Administration.

Change requests are reported to the WVFIMS support staff directly, through the personnel at the Finance Division, or through the WVOT service desk and are researched by the staff. If it is determined that a modification is required, staff management authorizes the programmer/analyst to address the problem by creating a Request for Data Processing Services (RDPS) with the programmer/analyst indicated as the assigned staff. The change request is documented in the RDPS and is forwarded to the appropriate individual(s) authorized to approve the change **(Control 1.2)**.

All requests, irrespective of how they were initiated or who initiated them, should end up on a RDPS. Enhancements to the System dictated by legislative change, policy change, or opportunity for a process improvement start as a RDPS being created and staff assigned to create a design document. This activity may not have an authorization, but the affected party or parties approve the design prior to staff being assigned to begin development. Some enhancement projects require authorization from multiple parties (e.g., an enhancement that requires a new posting rule would require authorization of both Finance and the State Treasurer's Office). Additionally, production fixes can be initiated by a Help Desk ticket, which would have been created at the onset of the problem, as documentation of the authorization of the change.

Testing of changes

WVOT maintains numerous CICS regions and DB2 sub-systems for the purpose of maintaining separate environments (i.e., unit test and system test) from production for development/testing purposes **(Control 1.3)**. The unit test environment is limited to the developers. The developer uses the unit test environment to verify that the code performs as expected, based on written user requirements. The system test environment is expanded to include the developer, the user/requestor, and possibly others involved in the change. In the system test environment, end-user testing is performed. Approval(s) indicating that testing has been successfully completed by the end-user(s) is obtained **(Control 1.4)**. If the change is an internally reported production or performance problem, WVFIMS support staff management and/or Finance Division staff will test the change. The system test environment is often populated with the exact or similar data from production so the requestor and/or Finance can test the scenario that prompted the change. With enhancements that affect the control agencies, these entities are included in the testing. Documentation of testing performed in the unit test and system test environments are retained for maintaining history and accountability to support the fix/request.

Approval of changes into production

Upon completion of testing, the programmer informs the WVFIMS support staff management that the change is ready for production migration. The WVFIMS support staff management reviews the testing results and ensures all necessary components are completed prior to change migration approval. If the program is ready for migration, the manager advises the programmer to enter the migration request. The change migration is invoked by the manager approving the migration request via the Command Language (CLIST) control tool. The migration is made either urgently or after hours by setting a parameter within the migration request. In either option the process utilizes an automated job scheduler. Access to initiate and approve change migrations to production is controlled by the CLIST change control tool; access has been restricted to only WVFIMS support staff management to approve changes **(Control 1.5)**. Once the migration for approval has been obtained, the code is automatically migrated into production at the next scheduled time. WVFIMS support staff management takes into account the impact of the migration on the system when choosing urgent versus after hours.

Segregation of duties within the change management process

Access to initiate and approve program migrations to production is accomplished by entering information into a CLIST procedure. The procedure notifies the approver within the WVFIMS support staff management that there is a migration awaiting approval. The developer provides management with the development check list and other required documentation prior to entering the program migration request. Access to approve changes within the CLIST is restricted to WVFIMS support staff management; no developers have the ability to migrate changes to production within the CLIST **(Control 1.6)**.

How emergency changes are handled

Depending on the severity of the emergency, the process is typically followed as a normal change request. The main exception is that the change would be migrated to production immediately instead of waiting for the scheduled time. WVFIMS support staff management make the assessment that no acceptable work around is available and that an urgent migration of changed code is necessary. When possible this decision is made through collaboration with Finance. If the decision impacts a controlling agency, they are informed if possible and appropriate.

System Software and Network Changes

WVOT has developed formal policies and procedures over System Software/Hardware Development and Maintenance process, as well as the Patch Management process **(Control 2.1)**.

Networking Devices

The WVOT networking group utilizes the Kiwi CatTools application for scheduling jobs related to the changes or backups of network device configuration files, including routers, switches and firewalls, and scheduling patches to the network. Cisco's Internetwork Operating System, or IOS, is the system software used by WVOT on network routers, switches, and firewalls. IOS version upgrades, found on the Cisco.com website are evaluated and deployed by network engineering on an as-needed basis, typically in response to a technical issue or to address potential security vulnerabilities or functionality issues. Modifications to the State's network infrastructure are engineered by the WVOT's network engineering design team in accordance with accepted industry standards. Network changes are driven by technology advancements, move/add/change requests, break/fix issues, and performance requirements.

All upgrades and patches are reviewed for any caveats and tested prior to being deployed. IOS upgrades are tested offline in a simulated network environment for functionality by the WVOT networking group **(Control 2.2)**. The testing center is appropriately locked and access is granted to only those requiring access.

Configuration changes can vary widely dependent upon the location and function of the device. Some devices are modified on a daily or weekly basis while others are not changed after the initial setup. The Kiwi CatTools is configured to automatically log and store the changes that have been made to any network device configuration file **(Control 2.3)**. When a change occurs, an email is automatically emailed to the network support group.

In the event that a roll back is needed, Kiwi CatTools has the ability to maintain a history of up to 50 configuration settings to restore to the desired date and time settings. Backup copies of configuration files are stored on a secondary server operated by WVOT. Copies are dated and archived anytime a configuration change is made. Files can be pulled from the server and loaded onto a replacement device via the Kiwi CatTools following an unsuccessful application of a change and/or catastrophic failure. Any problems encountered when applying changes to the networks are escalated via the Help Desk ticketing system.

Emergency changes follow the same process as noted above but testing and approvals are escalated quickly through the process. Approval is required for emergency changes before they are implemented in production.

Additionally, access to make configuration changes is restricted to users with the ability to Telnet to the network devices governed by Cisco's TACACS system. Access to make configuration changes is restricted to the network engineers via security permissions configured in TACACS **(Control 2.4)**.

Windows Patches

The WVOT Windows Configuration Management Team (CMT) is charged with the routine maintenance of its computing assets and strives to ensure that all Windows-based systems are systematically kept up-to-date with the latest security patches, software updates, and/or relevant drivers. The WVOT CMT utilizes Microsoft's Windows Server Update Services (SUS) to deploy the latest product updates to the Windows operating systems. System updates are released by Microsoft on the second Tuesday of each month. Microsoft then downloads critical and relevant patches to a dedicated server for review by a CMT staff. Once a staff reviews the patches available on the Windows SUS Server for system and/or application relevant patches, the authorization of the change is documented when it is pushed to the test machines for testing procedures. Policy states that for regular-cycle patches testing should be completed within five working days. Upon successful testing of the patch, infrastructure team management approves the change during the monthly operations meeting which is documented within the push to the production server by the implementer selecting 'Allow' or 'Disallow' for it to be downloaded **(Control 2.5)**.

Patches and service packs are applied to workstations and servers to remediate exposure to applicable security issues. For portable computers to receive critical and security patches/updates they must be connected to the agency network at least once every two weeks.

Requests for manual patching are submitted in writing and must be approved by the CMT. Responsibility for patching servers and/or systems specifically designated as being manually patched must be negotiated during the approval process.

Emergency Windows Patches

Notification of emergency or critical patch releases is through the SUS. If an exploitation of vulnerability occurs, or an update is deemed imminent the CMT follows the 'out-of-band' patch process. When this type of patch is released, the CMT accelerates the testing phase and schedules a deployment as soon as possible. Patches are applied only after testing and confirmation of readiness and appropriateness have been verified. The 'out-of-band' patches are to be tested and released within two working days per policy.

Mainframe

Changes to the mainframe are in the form of vendor supplied patches and upgrades. The systems programmer is responsible for identifying relevant upgrades or patches to the mainframe from the IBM website. Upon identifying available changes, they are reviewed for applicability and appropriateness. If the change is deemed relevant, the data center manager assigns the change to authorized individuals to begin the installation process. Once the change is authorized, testing of systems software is conducted in the systems test LPAR (Logical Partition) region, rather than in one of the two production LPARs.

The systems programmers and the data center manager are required to test changes to the mainframe environment prior to implementation into production **(Control 2.6)**. Upon successful completion of testing, a full system backup is performed prior to any changes to system software being moved to production. In the event a patch doesn't work when moved to production, the system is restored to the original state using the backup.

Prior to production, the changes are discussed during the data center systems weekly staff meeting. Risks associated with changes are discussed and documented in the data center weekly staff meeting minutes. Additionally, the data center manager reviews the testing results and approves the change for production within the data center weekly staff meeting **(Control 2.7)**.

Users and service desk personnel are notified in advance of any scheduled system changes. When emergency changes must be applied, the data center manager or his designee authorizes the change and the users and Service Desk personnel are notified as soon as practical to do so. A manually maintained log containing detail of each change (description, issues – if applicable, and implementer) are maintained in the SY.CHANGES dataset residing on the mainframe.

IBM's System Modification Program/Extended (SMP/E) is one proprietary tool used by the data center to collect and maintain detailed documentation about system software changes, version numbers, and releases. SMP is used to install and maintain software. It selects the proper levels of elements to be installed from a large number of potential changes, and it calls system utility programs to install the changes. SMP keeps records of the installed changes and allows the user to revert back to previous levels when necessary. Also, the data center maintains a list of software titles and version numbers that are available to agencies on the data center website. Access to these documents is restricted by user ID and password.

UNIX/LINUX

The UNIX (HP-UX, AIX) and LINUX operating systems in place support Oracle database servers for the State agencies. Additionally, the UNIX and LINUX operating system servers support some Web application servers. As such, all patches or upgrades to these systems are application or database driven and change management activities relative to these systems are controlled by the agency specific change management processes.

System Monitoring

WVOT has defined policies and guidelines for ensuring that network security and system performance issues are identified and escalated to resolution **(Control 3.1)**.

Operating System/Network/Database

The network engineering team uses the network monitoring applications "What's up Gold" (WUG) and HP Systems Insight Manager to monitor and record infrastructure and agency networking devices for up or down status. The WUG application performs monitoring specific to router and switch devices while the HP Systems Insight Manager is specific to the servers. The monitoring applications utilize real-time monitoring consoles and are configured to send an automatic e-mail alert to the service desk and appropriate network analysts when equipment status is down **(Control 3.2)**. WVOT has developed formal instructions and service descriptions that provide guidance to the network analyst when responding to alerts. If an event is noted that requires action, the WVOT escalates the issue to the appropriate personnel on the networking team for resolution. The networking team is responsible for documenting the disruption incident in the Help Desk ticket system **(Control 3.3)**.

The WVOT security operations center (SOC) monitors various devices to observe login events, failed login events, privilege abuse, excessive firewall denies, IDS alerts, application usage, vulnerability information, policy violations, and illegal software usage. The devices that the SOC monitors include, but are not limited to:

- Intrusion sensors
- HoneyPots
- Domain Controllers
- Other servers/devices

Mainframe

Reports are run daily using System Management Facilities (SMF) records from the enterprise server. All SMF records are placed on a tape each night and then incorporated into monthly files. Reports are generated using SMF records for monitoring and the systems programmer reviews them the following day (**Control 3.4**). The following is a listing of what the systems programmer reviews:

- Abnormal Gateway transactions
- Total CPU usage for all of the Gateway subsystems
- VM CPU usage for each partition
- Customer Information Control System (CICS) CPU time by region and the number of transactions by region

Unplanned Outages

WVOT has monitoring controls in place 24 hours a day, seven days a week to identify when an outage occurs, which enables WVOT to allocate the appropriate resources to minimize interruptions in service. Additionally, the Internet Service Provider (ISP) has controls in place to notify relevant on-call service desk technicians when outages are detected during off-peak hours.

Planned Outages

In the event that a network outage is premeditated, all users are informed via e-mail notification well in advance of the outage. Additionally, the outages are posted on the WVOT intranet SharePoint site to access at any given time.

Logical Access

WVOT has defined policies and guidelines for ensuring information systems are secure to meet their obligations for maintaining confidentiality on business processes, research data, or other proprietary data **(Control 4.1)**. Employees are required to sign this document annually. Additionally, WVOT has defined policies and guidelines regarding confidentiality on business processes, research data, or other proprietary data for Executive Branch agencies **(Control 4.2)**.

WVOT has developed formalized policies and procedures governing logical access as well as overall information security **(Control 4.3)**.

User Access Creation / Modification

Operating System/Network/Database

The WVOT enterprise server is secured using IBM's RACF security product. User IDs are defined in the WVOT's Customer Information Control System (CICS) application, Information Systems Definition System (ISDS). This is an in-house written program utilized by user agencies to define their mainframe users, RACF Coordinators, default Project Accounting System (PAS) numbers, and their data sets. Each agency is assigned a two character prefix; all user IDs for that agency begin with that prefix. Most agencies that have their own RACF coordinator also maintain their agency's user IDs, using their agency's policy. The WVOT account management group assigns RACF user IDs and either the service desk or account management group resets passwords in agencies without their own RACF coordinator and agencies electing to use WVOT's services. A list of all agencies and their RACF coordinators is maintained in a spreadsheet within the WVOT data center.

The WVOT account management group assigns network user IDs and either the service desk or account management group resets passwords for the WVOT Active Directory network. Each user is assigned a unique user ID, non-state employees requiring Network user IDs are designated by the 'C' prefix.

To have an account created or modified for the SQL Server access a request is submitted to the DBA responsible for that database. The DBA specifies the type of access to grant and obtains the relative approvals for the access. The approval must be requested from the designated agency contact or WVOT manager. There are some circumstances in which WVOT has given customers the ability to access data within Crystal reports. This is controlled through user access levels. Customized applications have a security module developed to allow an agency administrator to control access to the application. The WVOT makes recommendations, but ultimately the request process is then left up to the agency to define.

To gain access to the UNIX/LINUX operating system servers that support the Oracle databases, a request must be submitted to the UNIX/LINUX admin team lead. This is a rare occurrence as access to login to the servers is limited to a small user base within the UNIX/LINUX administration department.

New account requests and account modifications for the network, operating systems, and databases are submitted via account access forms that are initiated by the user or the user's manager; the form must be authorized (signature) by the approving manager or Designated Approval Authority (DAA) **(Control 4.4)**.

WVFIMS Application

A request for access to the WVFIMS application is initiated through either an e-mail or completion of the 'Request for Access to WVFIMS' form, and must be approved by the user's manager before access is granted **(Control 4.5)**. Requests for access may be received via e-mail, which is dependent upon individual agency policy. E-mail requests are only accepted from known authorized requestors. If a request for access is communicated verbally, the user must complete the "Request for Access to WVFIMS" form before the access is granted. Verbal requests are followed up by completing the request form or by e-mail. Some access requests (new or modifications) ask that a user be granted the same privileges as a specified existing user. It is the user's manager's responsibility to identify the access rights the individual requires to perform his/her job functions. The access request form or e-mail is then forwarded to the assistant to the support staff management who reviews the request and verifies that the approval authority is appropriate. If the access being requested is in question, the assistant calls the proper parties to obtain an understanding of why it is appropriate for the user to be granted the access. Once the access request is approved, a user profile is created within WVFIMS using the user's RACF ID. The ID must also be connected to the RACF group that grants access to the WVFIMS main menu transaction.

Standard user profiles vary based on job responsibilities the WVFIMS application. The dynamic nature of the menus enhanced security by only placing those transactions on a user's menu to which they are authorized or required to perform. When adding a new user, an existing menu (if an exact match exists) is assigned to that user. Users must have authorization by the requesting manager to obtain access to the appropriate transactions.

Any user who requires access modifications to their WVFIMS user profile is required to complete a "Request for Access to WVFIMS" form or submit an e-mail as described in the process above for the new user access.

User Access Removal

Requests for terminating employees follow the same process as new user creation. Once a user is terminated, a request is submitted by the designated agency contact or WVOT manager to the WVOT service desk. All system access is then removed for the terminated employee by the responsible administrators **(Control 4.6)**. Additionally, current Active Directory network settings allow for automatic disablement of network user IDs after 60 days of inactivity.

In addition, a report is e-mailed monthly to each RACF coordinator, advising them of any user IDs that have not been used in the past 150 days. The WVOT automatically deletes any user ID that has not been used in 180 days. E-mails are sent every week to each RACF coordinator notifying them of any employee separations based on information gathered from both the HRIS and PIMS systems and they are then responsible for determining if the inactive user ID should be deleted **(Control 4.7)**. Beyond PIMS e-mail notifications, a spreadsheet attachment is e-mailed to the service desk and client services to action accounts specific to their separations.

Periodic Review of User Access

WVFIMS Application

User access to the WVFIMS application is reviewed on an annual basis for appropriateness to ensure that access rights are commensurate with job responsibilities **(Control 4.8)**. The assistant to the support staff manager sends out a list of all users and their access to the appropriate business unit (BU) supervisors on an annual basis. Once reviewed and modified/confirmed, the BU supervisor sends a copy of the review back to the assistant to the support staff manager for any necessary revisions as a result of the review. WVOT does not perform a review of the access assigned to users outside of WVOT. WVOT only sends the agencies a system-generated listing of the access assigned to their users. Agency management is responsible for performing a review of user access on at least an annual basis to verify user access remains appropriate based on user job responsibilities.

Login Sequence / Password Parameters

To access the WVFIMS application or any other resources (i.e., operating system servers, databases) a user must first authenticate to the WVOT network via a unique user ID and password. Once authenticated to the network, the user accesses the application executable and must enter their RACF user ID and password to gain access to the WVFIMS application. WVOT policy related to security settings requires that access to all of the environments involve password and account management controls based on the technology used (**Control 4.9**) and include the following:

- Users are required to change their passwords periodically.
- User accounts are locked after a predetermined number of failed login attempts.
- User account passwords require a minimum length of characters.
- Users are prevented from reusing passwords previously utilized within a designated timeframe.

Passwords are reset by the WVOT service desk only after answering predetermined security questions, or by receiving a mainframe password reset request form signed by the agency's authorized requestor.

Privileged Access

Operating System/Network/Databases

Domain and Windows operating system server administrative accounts are restricted to network engineers and technicians within the WVOT and authorized outside partners **(Control 4.10)**. Depending on the hardware platform, users are authenticated via Access Control Server (ACS), which is the access control system for logging into the routers, switches, and WAN equipment, or through individual accounts created locally on the device.

SQL Server administrative access is restricted based on the individual's duties and is limited to WVOT DBAs and server administrators **(Control 4.11)**.

Administrator access to the UNIX/LINUX system administration privileges is limited to the WVOT UNIX/LINUX administrators **(Control 4.12)**.

Privileged access to user IDs and data is maintained by the RACF Coordinator and only at the agency level, based on the agency prefix. Universal access to production systems is limited to the WVOT Data Center systems programmers and access is required based on job responsibilities. RACF administrator privileges are limited to the WVOT and RACF coordinators based on job responsibilities **(Control 4.13)**.

WVFIMS Application

Administrator access to the WVFIMS application is restricted to a limited number of individuals within the WVFIMS support staff **(Control 4.14)**. These individuals require this level of access to create, modify, and terminate user accounts and also administer the application in the event emergencies arise.

Remote Access

Remote access to the WVOT network is restricted based on an individual's role. The server administrators and WVOT DBAs are granted remote access to the servers they support. If an agency owns a server, their server administrator and/or DBA are granted remote access. Remote access is provided on an as-needed basis and must be approved by a department manager on the new access form **(Control 4.15)**. Users must authenticate to the WVOT server via their network ID and password to access the remote network **(Control 4.16)**.

The mainframe enterprise server is accessed remotely using TPX, a VTAM session manager, which provides a consistent, secure point of entry to multiple, simultaneous mainframe applications. Many of the agencies accessing TPX use BlueZone terminal emulation software encrypted using SSL. Unique user IDs and passwords are required for login to the remote enterprise server and to perform specific functions **(Control 4.17)**.

Security Access Monitoring

Operating System/Network/Databases

Monitoring of RACF security violations are proactively reviewed and addressed on a routine basis by the RACF administrators **(Control 4.18)**. All RACF System Management Facilities (SMF) records are captured nightly and incorporated to a monthly file. Reports are generated daily using SMF records from the enterprise server for each agency. These RACF Security Violations reports detail login password failures, unauthorized attempts to administrator accounts, unauthorized attempts to agency-specific accounts, etc. These reports are reviewed by the RACF administrator. If more than five violations occur in a single day from a single user, an e-mail is sent to the agency specific RACF coordinator.

Monitoring of the network and servers is performed by utilizing the Dragon tool. The tool collects event logs from servers on security violations and compares the collected information to predetermined thresholds. Dragon is configured to perform real time monitoring by sending automated alerts when deviations from the predetermined limits or activities have occurred. Once a deviation is identified, the issue is escalated in the form of a Help Desk ticket and tracked to resolution **(Control 4.19)**.

Physical Access and Environmental Controls

WVOT has developed formal policies and procedures over physical access and environmental controls for the data center **(Control 5.1)**.

Data Center Facility and Networking Area

The WVOT data center site has evolved over time from a mainframe operations environment to a multi-purpose shared facility. In addition to data center employees and support engineers, access has been extended to some other WVOT personnel and some from other State agencies.

The WVOT data center is located at the Capitol Complex in Charleston, West Virginia. Access to this building is secured by an electronic card reader system and access provisioning is controlled by the State's Division of Protective Services. There are three separate rooms that house the production servers for the applications, all telecommunication and networking equipment, and the electrical and UPS power backup equipment. The computer rooms are each secured by a card reader entry system. The data center can only be accessed by personnel with a badge that is activated for the specified data center room indicated. Every card reader door access is automatically logged 24/7 and all activity is retained for one year. To gain access to the data center, a user's supervisor must provide a valid business purpose within an e-mail request to the data center manager. If an individual requires access to the data center, the requestor must sign a form, describing his/her responsibilities, prior to receiving an access card **(Control 5.2)**. The data center retains the signed form, and the individual is given a copy. This form describes many access responsibility points, including what to do if the access card is lost or becomes inoperable. The data center manager is notified of a user's termination by their supervisor and access to the data center is revoked in a timely manner **(Control 5.3)**.

Cameras located in the building hallways are maintained by General Services and monitored by Protective Services. The data center entrance is also equipped with a camera, which is maintained and monitored by data center personnel.

Access to the data center is restricted to authorized personnel who have authorization to operate, supervise, or provide maintenance to the area and its equipment **(Control 5.4)**. Individuals without pre-authorized card reader access to Building 6 are issued a visitor's badge to the main building. Upon entering the data center area, visitors must again sign-in and receive a data center visitor's badge **(Control 5.5)**. Visitors are escorted throughout the data center and to secured areas by designated WVOT personnel, and are accompanied at all times while they are within the facilities. Upon completion of the data center tour, visitors must return the badge and sign-out.

Data Center (Environmental Controls)

The WVOT data center is equipped with a variety of environmental control devices **(Control 5.6)**. The data center sits on a raised floor with water and smoke detection devices in the floor and ceiling. Heating Ventilation and Air Conditioning (HVAC) within the WVOT data center uses chilled water from the Capitol Complex chiller plant, which is maintained by General Service Division (GSD). There are seven chilled water air handlers, and one glycol-based air handler. WVOT maintains two pumps (primary and backup) along with a backup 50/60 ton dual chiller. The chillers are all controlled and monitored by software. The backup chiller system is exercised once a week for four hours. Software is used to monitor temperatures and other conditions (see below) and notify data center personnel if adverse conditions are triggered. The WVOT data center has a halon-based fire suppression system. The system will activate if smoke is detected independently by two or more sensors. Temperature/humidity monitoring software immediately notifies key personnel via pager of any unscheduled event.

The WVOT data center power is regulated through dual UPS units and dispersed through three power distribution units within the computer room. During a power failure, controls at the UPS automatically switch the power source to an external generator. The generator is exercised once a week. Monitoring software immediately notifies key personnel, via pager, of any unscheduled event.

The data center inspection schedule is as follows for the relative environmental equipment:

- All of the cooling equipment (chiller, pumps and air handlers) is under a maintenance contract and has a monthly inspection.
- The PDU's, UPS and Battery cabinets are under contract and have semi-annual inspections. The data center maintains and reviews the inspection results.
- The generator is under a maintenance contract and has quarterly inspections.
- The fire suppression equipment and the halon/dry sprinkler controls undergo annual inspection.

The data center maintains and reviews inspection results.

Printing/Distribution Area

The printing/distribution area is also located at the Capitol Complex. The area is secured, and access is restricted as described above.

Users receiving output from the printer area have designated output boxes that are secured by a key lock. Securing the data deposited in these boxes is the responsibility of the key-holders. The boxes are located in an alcove adjacent to the printer area. Computer operators place output into the boxes from within the secured room. The boxes open on the other side of the wall, into the alcove. To retrieve computer output, users must pick up their printouts, using their keys. Users are not allowed inside the room for the purpose of obtaining computer output. Computer operators are not permitted to retrieve user output from the boxes for any reason.

If an agency has a bulk print job, the computer operators place a notice in the particular output box. To retrieve the bulk print, the user must bring the notice from their agency's box to a specified location, and ring the buzzer. The computer operator will ask the user for the notice, and then give the bulk print to the user. Visitors are not allowed into the room to obtain bulk print. Agencies are not allowed to remove bulk print from the area without the appropriate notification form.

Automated Job Scheduling

Automated Job Scheduling – Data Center

The WVOT data center utilizes the Control-M job scheduler for batch job scheduling, which includes backups and WVFIMS related batch processing jobs. Control-M access is restricted by RACF security. Access to the job schedule is granted by a Control-M Administrator within the WVOT data center once requested by the agency authority. Access to the Control-M job schedule is limited to WVOT systems programmers, IT management, and agency representatives based upon job responsibilities **(Control 6.1)**. A list of all agencies and their RACF coordinators is maintained in a spreadsheet within the WVOT data center. The agency is responsible for monitoring their specific batch jobs for failures. Once prompted by the agency, the WVOT data center provides problem management support through resolution for agency failed jobs.

If a critical data center batch job fails, the Control-M system automatically notifies either the systems programmer on-call, or the person responsible for the job **(Control 6.2)**. There is one systems programmer on call 24/7. Each agency maintains their own procedures for their agency's job failures. This may include pages, e-mails, notifies or text messages to the on-call systems programmer.

The Control-M job schedule is monitoring the backup and processing jobs on a 24/7 basis **(Control 6.3)**. Every day a report is produced and monitored showing the results of all jobs scheduled by Control-M for the WVOT data center for the previous 24 hours. The report is maintained online for a minimum of 31 days. The report contains the schedule name, user ID, date, job name, job number, type, and results.

Automated Job Scheduling – Network

The WVOT networking group utilizes the Kiwi CatTools application for scheduling related to the changes or backups of network device configuration files, including routers, switches and firewalls, and scheduling patches to the servers. Access to the Kiwi CatTools job schedule is limited to network engineers and personnel responsible for configuration changes or patching the network devices **(Control 6.4)**. The schedule is planned to execute mass upgrades after normal business hours. In addition to the aforementioned abilities, the Kiwi CatTools allows the WVOT to generate network device configuration reports, such as port, media access control (MAC), and version details. The Kiwi CatTools is configured to automatically send the Director of Infrastructure Design and Operations an email when any configuration changes have been made to the network device configuration files. In the event that a roll back is needed, Kiwi CatTools has the ability to maintain a history of up to 50 configuration settings to restore to the desired date and time settings

Problem Management and Tracking

WVOT has defined policies and guidelines to address significant operations problems and to adequately report, escalate, track, and monitor through resolution **(Control 7.1)**.

The core service desk personnel are stationed at WVOT's service desk, located at the Capitol Complex in Charleston, WV. The service desk employs a staff of approximately 15 people. Other service desk personnel and field technicians are located at various regions/sites throughout the State. All service desk personnel and field technicians are required to complete HEAT Help Desk Software (HEAT) training, service desk procedures, and general IT orientation training. The problem resolution procedures are maintained on the SharePoint site. Service desk personnel utilize HEAT to track related issues/problems and requests to resolution and all incident calls are logged into the HEAT System **(Control 7.2)**. Each ticket, which is tracked through the system, contains the nature of the problem, call statistics, the contact, and any relevant notes. All incidents entered into HEAT are reviewed, prioritized, assigned to support personnel for resolution, and the current status is updated.

If the WVOT service desk cannot resolve the problem by phone or by remote control, the WVOT service desk assigns the ticket to the proper groups / personnel / field technicians, or the appropriate subject matter experts. At that time, a severity level is assigned to the ticket along with any additional necessary information. Severity levels are as follows:

- **Severity 1**: Critical, two business hours from time of trouble ticket receipt of incident trouble ticket to be contacted by a technician.
- **Severity 2**: Eight business hours from time of receipt of incident trouble ticket to be contacted by a technician.
- **Severity 3**: Two business days from time of receipt of incident trouble ticket to be contacted by a technician.
- **Severity 4**: Five business days from time of receipt of incident trouble ticket to be contacted by a technician.
- **Severity 5**: Non-critical, will resolve as time allows.

Once the ticket is resolved, an automatic e-mail is sent to the user to verify the closure. If customer contact has not been initiated by the identified severity levels, an e-mail is automatically generated and sent to the client services director. After a further specified amount of time has passed, an additional automatically generated e-mail will be sent to the CTO to alert them of the open ticket past contact time. In the case of an unplanned outage however, the CTO is immediately notified via an automatically generated e-mail.

Call statistics and problem tickets are tracked on a daily basis through HEAT to help ensure they are resolved in a timely manner. Daily outstanding ticket updates are automatically sent to team leads and managers to which the ticket belongs. Call statistics are compiled monthly by service desk team leads and managers and made available on the WVOT SharePoint site to compare against service level and escalation structures (**Control 7.3**). Comparison reports summarizing month to month call volumes, severity level of the ticket requests and escalation levels of tickets are provided to the CTO and each of their direct reports.

The WVOT service desk is fully staffed Monday through Friday from 7:00 a.m. to 5:00 p.m. and is also available 24 hours a day, 365 days a year by afterhours support **(Control 7.4)**. WVOT utilizes West Virginia Network (WVNET) to perform phone support after hours for the service desk. WVNET has the ability to perform a minimal level of services for the WVOT such as password resets and printer restarts. If there is an issue that the WVNET service cannot perform they escalate the problem to the on-call service desk staff member. The WVOT service desk requires at least two on-call technicians at all times during non-business hours.

Data Backup and Recovery

WVOT has defined policies and guidelines to provide reasonable assurance that programs, files, and datasets that have been identified as requiring periodic back-up are properly backed up and retained **(Control 8.1)**.

Data Backup

WVOT is currently in the implementation phase of a centralized consolidated backup solution. The WVOT over time has inherited multiple data centers, which were previously managed by individual State agencies. Each agency had its own data center or server room(s) and managed its own backup/recoveries with each data center having its own backup product and hardware. Additionally, some backups for the small servers located at county/regional offices had internal tape drives.

Mainframe

"Copy disks" make a copy of all data on the mainframe. WVOT utilizes the Control-M job scheduler for enterprise server system backups. The Control-M software is an automated system that submits batch jobs, which perform a weekly full volume backup in two phases on Sunday morning and Sunday evening on the mainframe, WVFIMS application and DB2 database (**Control 8.2**). These are made from disk to a tape system located at the secondary data center in Flatwoods, WV. There are at least two generations of copy disk tapes kept off-site at all times.

Network/Operating System and Mainframe

WVOT uses the Tivoli Storage Manager (TSM) and Avamar to back up selected Windows, NetWare, UNIX and LINUX file servers. TSM and Avamar are automated systems that back up selected portions of those file servers, on varying schedules (**Control 8.3**). All of the backup parameters are specified by the user and configured in TSM and Avamar by the responsible WVOT data center employees.

Other critical backups are taken daily and written on the tape system in Flatwoods. These have various expiration dates, with no vault tape being kept at One Davis Square longer than 30 days. Full system backup is a disk-to-tape backup of all data on mainframe peripheral disk storage subsystems at the data center. The data center takes this weekly backup for its own purposes. It is not a substitute for user-agency file backups. Agencies are responsible for backing up their files to tape. The data center has custodial responsibility for user-agency backup tapes.

Monitoring of Backups

The Control-M job schedule is configured to automatically notify the administrator via time sharing options (TSO) notifications and pages that a job has not completed successfully. All failures of backup jobs are escalated and resolved through the WVOT problem management process. The TSM and Avamar backups are monitored on a real-time basis for successful completion. The IS Manager monitors daily backups and reviews logs of both successes and failures. If any failures are discovered, the IS Manager notifies the agency involved, and takes appropriate steps to correct the failure **(Control 8.4)**. This may involve working with other area experts (communications, file servers, etc.) to take corrective action.

Recovery

If a dataset needs to be restored, the data is recovered from either a backup tape located in Flatwoods or from the disk backup located on the Avamar system or the virtual tape system. Disaster Recovery testing is done once a year in Philadelphia, PA to identify any problems and verify the environment can be restored **(Control 8.5)**.

WVOT uses the TSM and Avamar systems to ensure that requested agency mainframe data are properly backed-up and retained. Agency personnel make recovery requests via the service desk. Restore tests are performed on an as-requested basis by the agency **(Control 8.6)**.

Backup Schedule Configuration Changes

Backup schedule changes impacting the mainframe, WVFIMS application and DB2 database are initiated and performed by WVOT. Prior to making a backup schedule change, the change must be logged by the systems programmer in the mainframe dataset log by the system programmer and approved by the data center manager during the data center systems weekly staff meeting (**Control 8.7**). Risk associated with changes are discussed and documented in the data center weekly staff meeting minutes.

Backup copies of configuration files are stored on a secondary server operated by WVOT and copies of the changes are dated and archived anytime a configuration change is made. Files can be pulled from the server and loaded onto a replacement device following an unsuccessful application of a change and/or catastrophic failure. Configuration changes can vary widely depending upon the location and function of the device. Some devices are modified on a daily or weekly basis, while others may never need to be reconfigured.

Access to Backup Utilities

Access to make changes (i.e., add, modify, or delete backups jobs) to the TSM and Avamar backup schedules is restricted to those users with privileged access to the utilities (**Control 8.8**).

Control Objectives and Controls

The control objectives specified by WVOT and the controls that achieve those control objectives are listed in the accompanying *Description of Control Objectives, Controls, Tests and Results of Tests.*

Complementary User Entity Controls

In designing its system, WVOT has contemplated that certain complementary controls would be implemented by user organizations to achieve certain control objectives included in this report. The complementary user entity controls are listed in *Description of Control Objectives, Controls, Tests and Results of Tests.*

Description of Control Objectives, Controls, Tests and Results of Tests

Testing performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of our testing of the controls specified by WVOT, we considered the aspects of WVOT's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Control Objectives and Controls

On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by, and are the responsibility of, WVOT. The testing performed by Ernst & Young LLP and the results of tests are the responsibility of the service auditor.

Application Software Development

Control Objective #1

Controls provide reasonable assurance that application code and configuration parameter changes are initiated as needed, are authorized, and function in accordance with application specifications to (1) result in valid, complete, accurate and timely processing and data, (2) provide for the functioning of application controls, and (3) support segregation of duties.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
1.1	WVOT has developed a formalized policy/procedural document outlining the application change management process from initiation through completion.	Inspected the application change management policies and procedures of the WVOT to determine that there is a formal process to initiate and complete changes. No deviations noted.
1.2	The fix or request documented in the RDPS is then forwarded to the appropriate individual(s) authorized to approve the change.	For a sample of new or modified programs selected, inspected change request documentation (RDPS form) noting authorization of the change. No deviations noted.
1.3	WVOT maintains numerous CICS regions and DB2 sub-systems for the purpose of maintaining separate environments (i.e., unit test and system test) from production for development/testing purposes.	Inspected system documentation to determine that the program change control process for the WVFIMS application utilizes separate integrated test and production environments. No deviations noted.
1.4	Approval(s) indicating that testing has been successfully completed by the end-user(s) is obtained.	For a sample of new or modified programs selected, inspected program change documentation for testing completion and approval prior to implementation into production. No deviations noted.
1.5	Access to initiate and approve change migrations to production is controlled by the CLIST change control tool; access has been restricted to only WVFIMS support staff management to approve changes.	For a sample of new or modified programs selected, inspected documentation noting that approval was obtained prior to the programs being placed into production. No deviations noted.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
1.6	Access to approve changes within the CLIST is restricted to WVFIMS support staff management; no developers have the ability to migrate changes to production within the CLIST.	Through inspection of the users with access to the CLIST, assessed the appropriateness of access of migrating changes to production to determine that it is restricted to personnel not responsible for development activities. No deviations noted.

Complementary User Entity Controls

- User organizations should have processes in place to ensure that end users are appropriately notified of possible application changes, as to allow for proper testing of changes prior to implementation.
- User organizations should have controls in place to ensure that only authorized user organization personnel can request or authorize WVOT to make changes to their environment.
- User organizations are responsible for authorizing and accepting all changes to their applications and, therefore, should ensure appropriate change control policies and procedures are in place.

System Software and Network Changes

Control Objective #2

Controls provide reasonable assurance that network infrastructure is configured as authorized to (1) enable applications and application controls to operate effectively, (2) protect data from unauthorized changes and provide for its availability for processing, and (3) support segregation of duties.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
2.1	WVOT has developed formal policies and procedures over system software/hardware development and maintenance process, as well as the patch management process.	Inspected the system software/hardware development and maintenance, including patch management, policies and procedures of the WVOT, to determine that there is a formal process to initiate and apply changes/patches. No deviations noted.
2.2	IOS upgrades are tested offline in a simulated network environment for functionality by the WVOT networking group.	Performed a physical walkthrough of the simulated network environment testing lab and verified that the entrance was secured to only authorized users. Additionally, validated that testing equipment was separated from the production network and servers where testing is performed prior to production implementation. No deviations noted.
2.3	The Kiwi CatTools is configured to automatically log and store the changes that have been made to any network device configuration file.	Inspected system documentation from Kiwi CatTools to verify all changes are logged and the change details are maintained within separate text files based on the category of the network device (Access Points, Firewalls, Routers, and Switches). No deviations noted.
2.4	Access to make configuration changes is restricted to the network engineers via security permissions configured in TACACS.	Inspected system documentation from TACACS to verify access is appropriately restricted to network engineers. No deviations noted.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
2.5	Upon successful testing of the patch, infrastructure team management approves the change during the monthly operations meeting which is documented within the push to the production server by the implementer selecting 'Allow' or 'Disallow' for it to be downloaded.	For a sample of upgrades/patches selected, inspected documentation to determine that the update/patch was properly approved and pushed to the production server for implementation into production. No deviations noted.
2.6	The systems programmers and the data center manager are required to test changes to the mainframe environment prior to implementation into production.	For a sample of mainframe changes selected, inspected documentation noting testing was completed prior to being implemented into production. No deviations noted.
2.7	The data center manager reviews the testing results and approves the change for production within the data center weekly staff meeting.	For a sample of mainframe changes selected, inspected the data center weekly staff meeting minutes noting approval of the data center manager was obtained prior to being implemented into production. No deviations noted.

Complementary User Entity Controls

- User organizations should ensure that releases of patches and upgrade software on workstations, terminals and client networks, including utilities and tools, are supported by the vendor.
- User organizations should have processes in place to ensure that end users are appropriately notified of possible system software and network changes, as to allow for proper testing of changes prior to implementation.
- User organizations should have controls in place to ensure that only authorized user organization personnel can request or authorize WVOT to make changes to their environment.
- User organizations are responsible for authorizing and accepting all changes to their environment and, therefore, should ensure appropriate change control policies and procedures are in place.

System Monitoring

Control Objective #3

Controls provide reasonable assurance that networks are monitored for availability and response times, and issues are documented and tracked until resolved.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
3.1	WVOT has defined policies and guidelines for ensuring that network security and system performance issues are identified and escalated to resolution.	Inspected the network security/monitoring policies and procedures of the WVOT to verify network issues are identified and escalated to resolution. No deviations noted.
3.2	The monitoring applications utilize real-time monitoring consoles and are configured to send an automatic e-mail alert to the service desk and appropriate network analysts when equipment status is down.	Inspected network monitoring applications utilized for infrastructure and agency networking devices for up or down status real-time. Additionally, inspected the monitoring applications for configuration to send an email notification to the network engineering team based on pre-determined criteria. No deviations noted.
3.3	The networking team is responsible for documenting the disruption incident in the Help Desk ticket system.	Refer to testing procedures performed and results of tests for control **7.2**.
3.4	SMF generates reports for monitoring and the systems programmer reviews them the following day.	For a sample of days within the audit period, inspected SMF reports and noted security monitoring review is performed daily by the systems programmer. No deviations noted.

Logical Access

Control Objective #4

Controls provide reasonable assurance that access to system resources, including computing platforms, operating systems and databases is restricted to properly authorized individuals.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
4.1	WVOT has defined policies and guidelines for ensuring information systems are secure to meet its obligations for maintaining confidentiality on business processes, research data, or other proprietary data.	Inspected the information systems policies and guidelines of the WVOT to determine that there is a formal process to ensure information systems and data are secured. No deviations noted.
4.2	WVOT has defined policies and guidelines regarding confidentiality on business processes, research data, or other proprietary data for Executive Branch agencies.	Inspected the confidentiality data policies and guidelines of the WVOT to determine that there is a formal process to protect sensitive information. No deviations noted.
4.3	WVOT has developed formalized policies and procedures governing logical access, as well as overall information security.	Inspected the logical access policies and procedures of the WVOT to determine that logical access and information security are restricted to authorized individuals. No deviations noted.
4.4	New account requests and account modifications for the network, operating systems, and databases are submitted via account access forms that are initiated by the user or the user's manager; the form must be authorized (signed) by the approving manager or Designated Approval Authority (DAA).	For a sample of new/modified account requests to the network, operating systems, and databases, inspected user access request documentation to determine that it was submitted via account access forms and contained the required approvals. No deviations noted.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
4.5	A request for access to the WVFIMS application is initiated through either an e-mail or completion of the "Request for Access to WVFIMS" form, and must be approved by the user's manager before access is granted.	For a sample of requests for access to the WVFIMS application, inspected documentation to determine that the request was authorized and approved. Additionally, verified the requested access, as documented in the form, was set up within the WVFIMS application. Deviation noted. Out of twenty-five WVFIMS users tested with newly created or modified access, four users did not have supporting documentation maintained to evidence that the access was approved by their manager. Management Response: While formal documentation did not exist for four of the sample selections, based on inquiry with the agency users' manager, each of the users' WVFIMS application access accounts is appropriate and in accordance with their job responsibilities. Further, in order to add or modify WVFIMS application access, a user has to have administrator access which is appropriately restricted.
4.6	All system access is removed for the terminated employees by the responsible administrators.	For a sample of terminated users, inspected documentation noting access to the systems was removed in a timely manner. No deviations noted.
4.7	E-mails are sent every week to all RACF coordinators notifying them of any employee separations based on information gathered from both the HRIS and PIMS systems and they are then responsible for determining if the inactive user ID should be deleted. Beyond PIMS e-mail notifications, a spreadsheet attachment is e-mailed to the service desk and client services to action accounts specific to their separations.	For a sample of weeks within the audit period, inspected e-mails sent to RACF coordinators for the selected weeks and determined that notification was provided and terminated employees were deleted. No deviations noted.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
4.8	User access to the WVFIMS application is reviewed on an annual basis for appropriateness to ensure that access rights are commensurate with job responsibilities.	Inspected the annual WVFIMS periodic review to determine WVOT specific user access to the WVFIMS application is reviewed on an annual basis and approved by WVOT management. Selected a sample of access modifications/deletions and verified that access was updated as noted within the review. No deviations noted.
4.9	WVOT policy related to security settings requires that access to all of the environments involve password and account management controls based on the technology used.	Inspected the network password settings for establishment in accordance with industry leading practices. No deviations noted. For a sample of Windows operating system servers, inspected the local server password settings for establishment in accordance with industry leading practices. No deviations noted. For the mainframe environment that also governs access to WVFIMS, inspected the RACF security password settings for establishment in accordance with industry leading practices. No deviations noted. For a sample of SQL databases, inspected the local server password settings for establishment in accordance with industry leading practices. No deviations noted. For a sample of UNIX and LINUX operating system servers, inspected the server password settings for establishment in accordance with industry leading practices.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
		Deviation noted. For the six UNIX operating system servers sampled, the password settings were not consistently configured with industry leading practices on the servers. Specifically: • Two of the servers did not have minimum length, account lockout, or password history configured. • Three of the servers did not have minimum length, account lockout, password expiration, or password history configured. • One of the servers did not have minimum length or password history configured. For the two LINUX operating system servers sampled, the password settings (password expiration and history) were not configured on the servers. Management Response: Although password settings are not configured with industry leading practices, a password is required to access each of the servers and authentication to the WVOT network is required as part of the logon sequence. Additionally, only administrators are logging directly into the operating system servers with inadequate password settings; administrator access was determined to be appropriately restricted on each of the servers.
4.10	Domain and Windows operating system server administrative accounts are restricted to network engineers and technicians within the WVOT, and authorized outside partners.	Inspected network privileged users and determined if access was restricted to authorized users based on job responsibilities. For a sample of Windows operating system servers, inspected privileged access accounts and groups to determine if access is appropriately restricted to authorized users based on job responsibilities. No deviations noted.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
4.11	SQL Server administrative access is restricted based on the individual's duties and is limited to WVOT DBAs and Server Administrators.	For a sample of SQL databases, inspected privileged access accounts and security settings to determine if access is appropriately restricted to authorized users based on job responsibilities. No deviations noted.
4.12	Administrator access to the UNIX/LINUX system administration privileges is limited to the WVOT UNIX/LINUX administrators.	For a sample of UNIX and LINUX operating system servers, inspected privileged access accounts and security settings to determine if access is appropriately restricted to authorized users based on job responsibilities. No deviations noted.
4.13	RACF administrator privileges are limited to the WVOT and RACF coordinators based on job responsibilities.	Inspected user documentation and determined that access to RACF administrator privileges are appropriately restricted to WVOT and RACF coordinators based on job responsibilities. No deviations noted.
4.14	Administrator access to the WVFIMS application is restricted to a limited number of individuals within the WVFIMS support staff.	Inspected user documentation and determined that administrator access to the WVFIMS application is appropriately restricted to authorized WVFIMS support staff based on job responsibilities. No deviations noted.
4.15	Remote access is provided on an as-needed basis and must be approved by a department manager on the new access form.	For a sample of users that have gained access to the remote network, verify that they had an access form submitted and that it was approved by a department manager. No deviations noted.
4.16	Users must authenticate to the WVOT server via their network ID and password in order to access the remote network.	Refer to testing procedures performed and results of tests for control **4.9**.
4.17	Unique user IDs and passwords are required for login to the remote enterprise server and to perform specific functions.	Inspected system settings to validate unique user IDs and password settings are required for the remote enterprise server. No deviations noted.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
4.18	Monitoring of RACF security violations is proactively reviewed and addressed on a routine basis by the RACF administrators.	For a sample of days, inspected RACF security violations documentation and noted the security reports were reviewed by RACF administrators and noted violations are tracked and monitored. No deviations noted.
4.19	Dragon is configured to perform real time monitoring by sending automated alerts when deviations from the predetermined limits or activities have occurred. Once a deviation is identified, the issue is escalated in the form of a Help Desk ticket and tracked to resolution.	Obtained and inspected network security monitoring documentation and determined Dragon is configured to perform real time continuous monitoring on the network. Additionally, inspected deviation documentation and noted tickets were closed and resolved after Dragon alerted appropriate personnel. No deviations noted.

Complementary User Entity Controls

- User organizations that support their own applications should have policies and procedures in place for adding, modifying, and removing user accounts.
- User organization management should perform a review of user access on at least an annual basis to verify user access remains appropriate based on user job responsibilities.
- Customized applications have a security module that is developed to allow a user organization administrator to control access to the application. The user organization administrator is determined by the user organization.
- Procedures should be established to prohibit the use of shared user IDs or user IDs where passwords are not changed on a regular basis.
- User organizations are responsible for timely notification of terminations to WVOT.

Physical Access and Environmental Controls

Control Objective #5

Controls provide reasonable assurance that physical access to computer equipment, storage media and program documentation is restricted to properly authorized individuals and equipment and facilities are protected from damage by fire, flood or other environmental hazards.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
5.1	WVOT has developed formal policies and procedures over physical access and environmental controls for the data center.	Inspected the physical and environmental security policies and procedures for the WVOT to determine that there is a formal process around safeguarding and securing assets. No deviations noted.
5.2	To gain access to the data center, a user's supervisor must provide a valid business purpose within an e-mail request to the data center manager. If an individual requires access to the data center, the requestor must sign a form, describing his/her responsibilities, prior to receiving an access card.	For a sample of new/existing badges granted access to the WVOT data center, determined that access to the data center was authorized via a request to the data center manager and appropriate given job responsibilities/duties. No deviations noted.
5.3	The data center manager is notified of a user's termination by his/her supervisor and access to the data center is revoked in a timely manner.	For a sample of terminated users, inspected the WVOT data center access listing to review that terminated employees' access was removed from the data center. No deviations noted.
5.4	Access to the data center is restricted to authorized personnel who have authorization to operate, supervise, or provide maintenance to the area and its equipment.	For a sample of employees with access to the data center, determined that access to the data center was appropriate given job responsibilities/duties. No deviations noted.
5.5	Upon entering the data center area, visitors must again sign in and receive a data center visitor's badge.	For a sample of days within the audit period, inspected the visitor's log noting that visitors were required to sign in and sign out upon accessing the WVOT data center. No deviations noted.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
5.6	The WVOT data center is equipped with a variety of environmental control devices.	Performed a physical walkthrough and determined that the WVOT data center is equipped with a variety of environmental control devices. No deviations noted.

Automated Job Scheduling

Control Objective #6

Controls provide reasonable assurance that processing is appropriately authorized and scheduled and that deviations from scheduled processing are identified and resolved.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
6.1	Access to the Control-M job schedule is limited to WVOT systems programmers, IT management, and agency representatives based upon job responsibilities.	Inspected system access listing and determined that administrator access to the Control-M job schedule is granted to appropriate users based on job responsibilities. No deviations noted.
6.2	If a critical data center batch job fails, the Control-M system automatically notifies either the system's programmer on-call or the person responsible for the job.	For a sample of days within the audit period, reviewed system report and activity log to validate that the Control-M system automatically monitors the jobs for successful completion. In the event of failures, the system automatically notifies the designated individual. No deviations noted.
6.3	The Control-M job schedule is monitoring the backup and processing jobs on a 24/7 basis.	Refer to testing procedures performed and results of tests for control **6.2**.
6.4	Access to the Kiwi CatTools job schedule is limited to network engineers and personnel responsible for configuration changes or patching the network devices.	Inspected system access listing of users to the Kiwi CatTools schedule and determined if access was appropriately restricted based on job responsibility. No deviations noted.

Complementary User Entity Controls

- Access to the Control-M job schedule for each of the user organizations is assigned to RACF coordinators. The RACF coordinators are responsible for administering (adding, modifying, or deleting jobs) their job schedule.
- Changes to the user organization job schedules follow change management processes established at each of the user organizations and are not the responsibility of WVOT. Any additions, modifications or deletions to the job schedule are handled at the user organization level.
- Each user organization maintains its own procedures for its job failures.

Problem Management and Tracking

Control Objective #7

Controls provide reasonable assurance that significant operations problems are adequately reported, tracked and monitored through resolution.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
7.1	WVOT has defined policies and guidelines to address significant operations problems adequately and to report, escalate, track and monitor through resolution.	Inspected operation problem management and escalation policy and guidelines of the WVOT to determine that there is a formal process to address, report, and resolve incidents/problems. No deviations noted.
7.2	Service desk personnel utilize HEAT to track related issues/problems and requests to resolution, and all incident calls are logged into the HEAT System.	For a sample of closed Help Desk tickets within the audit period, inspected the tickets to determine that the problems/incidents were documented and resolved timely. No deviations noted.
7.3	Call statistics are compiled monthly by service desk team leads and managers and made available on the WVOT SharePoint site to compare against service level and escalation structures.	For a sample of months, inspected call statistics report to validate the report captures relevant and appropriate service statistics that management provides to WVOT staff. No deviations noted.
7.4	The WVOT service desk is fully staffed Monday through Friday from 7:00 a.m. to 5:00 p.m. and is also available 24 hours a day, 365 days a year by afterhours support.	Through inquiry and inspection of the WVOT Service Level Definitions and Objectives and the contract for off-hours services/support, determined that the WVOT service desk is staffed at all times (24 hours a day, 7 days a week). No deviations noted.

Data Backup and Recovery

Control Objective #8

Controls provide reasonable assurance that programs, files and datasets that have been identified as requiring periodic backup are properly backed up and retained.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
8.1	WVOT has defined policies and guidelines to provide reasonable assurance that programs, files and datasets that have been identified as requiring periodic backup are properly backed up and retained.	Inspected backup and retention policy and procedure document for the WVOT to determine that there is a formal process to back up and retain required programs, files and datasets. No deviations noted.
8.2	The Control-M software is an automated system that submits batch jobs, which perform a weekly full volume backup in two phases on Sunday morning and Sunday evening on the mainframe, WVFIMS application and DB2 database	Inspected Control-M backup utility and noted that the system is scheduled to run a weekly backup in phases each Sunday for the mainframe, WVFIMS application and DB2 database. No deviations noted.
8.3	TSM and Avamar are automated systems that back up selected portions of those file servers, on varying schedules.	Inspected TSM and Avamar job schedules and noted that the systems are scheduled to perform backups on a daily basis across the various clients/platforms. No deviations noted.
8.4	The IS Manager monitors daily backups and reviews logs of both successes and failures, and notifies the appropriate contact if a backup has not completed successfully. If any failures are discovered, the IS manager notifies the agency involved, and takes appropriate steps to correct the failure.	Refer to testing procedures performed and results of tests for controls **6.2** and **6.3** related to Control-M scheduled backups. For a sample of days within the audit period, inspected system documentation (from TSM and Avamar) to validate that backups were completed successfully and the tools are configured for automatic notification of backup status. Also, for backups that did not complete successfully, reviewed the steps taken to correct and document the incident/failure. No deviations noted.

	Key Controls Specified by WVOT	Testing Performed and Results of Tests
8.5	Disaster recovery testing is done once a year in Philadelphia, PA to identify any problems and verify the environment can be restored.	Through inquiry and inspection of the test results, determined that the annual disaster recovery test was successfully performed within the audit year. No deviations noted.
8.6	Restore tests are performed initially when a new backup process is initiated, and afterward on an as-requested basis by the agency.	For a sample of requested restores, obtained and inspected file restore documentation and noted that restore tests are performed and completed on an as-requested basis. No deviations noted.
8.7	Prior to making a backup schedule change, the change must be logged by the systems programmer in the mainframe dataset log by the system programmer and approved by the data center manager during the data center systems weekly staff meeting.	For a sample of changes made to the Control-M schedule, inspected documentation to validate that changes were captured within the dataset log and approved by the data center manager prior to being implemented into production. No deviations noted.
8.8	Access to make changes (i.e., add, modify, or delete backups jobs) to the TSM and Avamar backup schedules is restricted to those users with privileged access to the utilities.	Inspected system user documentation and determined that administrator access to the TSM and Avamar utilities is appropriately restricted to authorized users based on job responsibilities. No deviations noted.

Complementary User Entity Controls

- Each user organization is responsible for scheduling/conducting test restores for recovery purposes. WVOT personnel are available by request to assist with test restores.
- Each user organization is responsible for setting up a backup schedule maintaining its backups and the schedule.

Other Information Provided by WVOT

Glossary

Advanced Encryption Standard (AES) – A single key encryption standard authorized by NIST. It has key sizes of 128, 192, and 256 bits.

Agencies – Agencies within the Executive Branch of the West Virginia State government.

American Institute of Certified Public Accountants (AICPA) – The national professional association of Certified Public Accountants in the United States. It sets ethical standards for the profession and U.S. auditing standards for audits of private companies; federal, state and local governments; and non-profit organizations.

Applications Development Center (ADC) – Provides application software development and support to State agencies.

Automatic Call Distributor (ACD) – A device or system that distributes incoming calls to a specific group of terminals that agents use. It is often part of a computer telephony integration (CTI) system.

Capitol Complex – WVOT's physical location in Charleston, WV.

Central Processing Unit (CPU) – The portion of a computer system that carries out the instructions of a computer program, and the primary element carrying out the computer's functions.

Chief Information Security Officer (CISO) – Person designated by the CTO to oversee information security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.

Chief Technology Officer (CTO) – The person responsible for the State's information resources.

Computer Telephony Integration (CTI) – Technology that allows interactions on a telephone and a computer to be integrated or coordinated.

Configuration Management Team (CMT) – Charged with the routine maintenance of its computing assets and strives to ensure that all Windows based systems are systematically kept up-to-date with the latest security patches, software updates, and/or relevant drivers.

Consolidated Public Retirement Board (CPRB) – Responsible for the administration of all State retirement plans for educational employees, public employees, deputy sheriffs, judges, and public safety personnel with the exclusion of some higher educational plans. Although the Consolidated Public Retirement Board administers many retirement systems, the assets and administration of each system remain separate and distinct.

Customer Information Control System (CICS) – An IBM acronym for their online transaction server.

Customer Relationship Manager (CRM) – An agency's advocate within the West Virginia Office of Technology (WVOT) to ensure technical requirements are met and prioritized within WVOT.

Database Administrator (DBA) – An individual who is responsible for the design, implementation, maintenance and repair of an organization's database. The role includes the development and design of database strategies, monitoring and improving database performance and capacity, and planning for future expansion requirements.

Department of Administration (DOA) – Responsible for implementing fiscal and administrative policies in the Executive Branch division and agencies. Oversees the Finance, General Services, Office of Technology, Personnel and Purchasing Divisions.

Designated Approval Authority (DAA) – Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Direct Access Storage Device (DASD) – In mainframe computers and some minicomputers, a DASD is any secondary storage device which has relatively low access time for all its capacity.

Division of Personnel (DOP) – A division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq.*, which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

Employee Performance Appraisals (EPA) – The purpose of the EPA is to establish a uniform performance appraisal system for State employees. During the performance appraisal, the agency identifies, measures, and evaluates an employee's job-related behaviors and accomplishments during a specific period of time and compares those to formerly established performance standards. Based on these comparisons, the agency can make judgments regarding an employee's strengths and weaknesses, and what can be done to enable the employee to perform more effectively.

Equal Employment Opportunity Office (EEO) – Established to prevent and eliminate unlawful employment discrimination and to promote diversity in West Virginia state government.

Financial Information Management System (FIMS) – The State's accounting system. WVOT has a role in the care and maintenance of the Administration's side of the system.

General Services Division (GSD) – The Division is comprised of several units, which provide operations and maintenance, architectural and engineering, asbestos coordination, health and safety coordination, custodial services and grounds maintenance for the West Virginia State Capitol Complex, and all buildings owned and maintained by the Department of Administration. In addition, General Services coordinates scheduling of events held on the State Capitol grounds.

Governor's Executive Information Security Team (GEIST) – Under the authority established by Senate Bill 653, effective July 1, 2006, and the Governor's Executive Order 06-06, and following the mandate of these documents, a Senior Information Security Team, known as the Governor's Executive Information Security Team (GEIST), has been put into place to assist with the implementation of Information Security initiatives throughout the Governor's Executive Branch.

Heating Ventilation and Air Conditioning (HVAC) – HVAC systems control the environment (temperature, humidity, air flow, and air filtering) and must be planned for and operated along with other data center components such as computing hardware, cabling, data storage, fire protection, physical security systems and power.

Helpdesk Expert Automation Tool (HEAT) – A commercial help desk software suite used to track, update, and close customer service requests.

Human Resource Information System (HRIS) – A software or online solution for the data entry, data tracking, and data information needs of the Human Resources, payroll, management, and accounting functions. HRIS provides overall management of all employee information, reporting and analysis of employee information, company-related documents such as employee handbooks, emergency evacuation procedures, and safety guidelines, benefits administration including enrollment, status changes, and personal information updating, complete integration with payroll and other company financial software and accounting systems, and applicant and resume management. HRIS can track attendance, pay raises and history, pay grades and positions held, personal employee information, etc.

Information Security Administrator (ISA) – The person designated by the agency head to assure the agency's compliance with State information security policies and procedures. The ISA is the agency's internal and external point of contact for all information security matters.

Information Technology (IT) – The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.

Internet Protocol Telephony (IPT) – A general term for the technologies that use the Internet Protocol's packet-switched connections to exchange voice, fax, and other forms of information that have traditionally been carried over the dedicated circuit-switched connections of the public switched telephone network (PSTN).

Internet Service Provider (ISP) – A company that offers its customers access to the Internet. The ISP connects to its customers using a data transmission technology appropriate for delivering Internet Protocol datagrams, such as dial-up, DSL, cable modem, wireless or dedicated high-speed interconnects.

Internetworking Operating System (IOS) – Cisco system software used by WVOT on network routers, switches, and firewalls.

IS&C Definition System (ISDS) – An in-house written program for defining user IDs. It actually uses CICS to do so.

Learning Management System (LMS) – A system used by the WVOT to deliver and track online training.

Logical Partition (LPAR) – A subset of computer's hardware resources, virtualized as a separate computer. In effect, a physical machine can be partitioned into multiple LPARs, each housing a separate operating system.

Media Access Control (MAC) – A data link layer protocol that provides addressing and channel access control mechanisms, which make it possible for several terminals or network nodes to communicate within a multi-point network.

Memorandum of Understanding (MOU) – A document describing a bilateral or multilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action.

Multi-Protocol Label Switching (MPLS) – A mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols.

Office of Information Security and Controls (OISC) – The functional unit charged with the responsibility to undertake and sustain initiatives to promote, enhance, monitor, and govern actions, standards, and activities necessary to safeguard data and information systems within the Executive Branch of WV, as provided in West Virginia Code §5A-6-4a.

Personally Identifiable Information (PII) – Includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact an individual.

Position Information Management System (PIMS) – The PIMS system reflects positions within all agencies of State Government. This system tracks Employee Personal Information, Employee History Information and current funding information for Positions. This system also processes the WV11 transactions that occur for employees, such as promotions, reallocations, funding source changes.

Power Distribution Unit (PDU) – A device that distributes electric power. Large industrial units are used or taking high voltage and current and reducing it to more common and useful levels.

Project Management Body of Knowledge (PMBOK) – A project management guide, and an internationally recognized standard, that provides the fundamentals of project management as they apply to a wide range of projects, including construction, software, engineering, automotive, etc.

Project Management Office (PMO) – Created by the Chief Technology Officer as directed by West Virginia Code §5A-6-4b. The PMO is responsible for managing information technology projects and providing oversight for state agency information technology projects.

Protected Health Information (PHI) – Health information transmitted by or maintained in electronic media used to identify an individual, which is created, used, or disclosed in the course of providing health care services such as diagnosis or treatment. Examples include: names, phone numbers, medical record numbers, photos, etc.

Public Employees Insurance Agency (PEIA) – Provides hospital, surgical, group major medical, prescription drug, group life, and accidental death and dismemberment insurance coverage to eligible employees; and establishes and promulgates rules for the administration of these plans. Benefits are made available to all active employees of the State of West Virginia and various related State agencies and local governments.

Request for Data Processing Services (RDPS) – Request system used by Information Services to initiate application development services.

Secure Socket Layer (SSL) – Cryptographic protocol that provides security for communications over networks such as the Internet. SSL encrypts the segments of network connections at the Transport Layer end-to-end.

Security Operations Center (SOC) – The WVOT SOC utilizes a set of tools that view events, correlate events that have known malicious signatures, or anomalous characteristics, and intervene when traffic or events suggest that some errant or malicious activity is taking place in the State network environment. When a problem is suspected, recorded logs can be used to analyze event history, and the cause can be identified to a point in time and often to a source location. Security Operations includes the SOC activities, as well as vulnerability scanning of State systems, validating patch levels, configuration hardening, and other system safeguards.

Service Level Agreement (SLA) – A service contract where the level of service is formally defined.

Software Update Services (SUS) – A free patch management tool provided by Microsoft to help network administrators deploy security patches more easily.

State Auditor's Office (SAO) – Serves as the State's official bookkeeper, Chief Inspector and Supervisor over Public Offices, Securities Commissioner and Commissioner of Delinquent and Non-entered Lands.

State Treasurer's Office (STO) – Serves as the State's banker and chief investment officer, processes the State's monies and pays all of the State's bills.

System Management Facilities (SMF) – A component of IBM's z/OS for mainframe computers, providing a standardized method for writing out records of activity to a file (or data set to use a z/OS term).

System Modification Program/Extended (SMP/E) – The basic tool for installing and maintaining software in z/OS and OS/390 systems and subsystems.

Terminal Productivity Executive (TPX) – TPX Session Management acts as the broker between you and your Virtual Telecommunications Access Method (VTAM) applications. By providing a single network connection to establish multiple concurrent sessions, it creates virtual sessions to applications as needed while offering the tools necessary for multitasking, session switching, connectivity, system management and communication.

Technology Learning Center (TLC) – Offers classes for various software packages supported on the personal computer to support State agencies in their day-to-day office automation needs.

Tivoli Storage Manager (TSM) – A centralized, policy-based, enterprise class, data backup and recovery software.

Uninterruptible Power Supply (UPS) – Provides emergency power to a load when the input power source fails.

Virtual Private Network (VPN) – A virtual computer network that exists over the top of an existing network. The purpose of a VPN is to allow communications between systems connected to the VPN using an existing shared network infrastructure as the transport, without the VPN network being aware of the existence of the underlying network backbone or without the VPN interfering with other network traffic on the backbone.

Voice over Internet Protocol (VoIP) – A general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Other terms synonymous with VoIP are *IP telephony*, *Internet telephony*, *voice over broadband* (VoBB), *broadband telephony*, and *broadband phone*. Internet telephony refers to communications services - voice, facsimile, and/or voice-messaging applications - that are transported via the Internet, rather than the public switched telephone network.

Wireless Area Network (WAN) – A computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations.

West Virginia Network (WVNET) – A service organization providing telecommunications and computing services within West Virginia.

West Virginia Office of Technology (WVOT) – The division of the Department of Administration established by WV Code § 5A-6-4a*, et. seq.,* which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

What's Up Gold (WUG) – A monitoring and management solution, designed to manage networks of all sizes.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: FAR140001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[ ] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

____
Company

____
Authorized Signature

____
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 6/8/2012