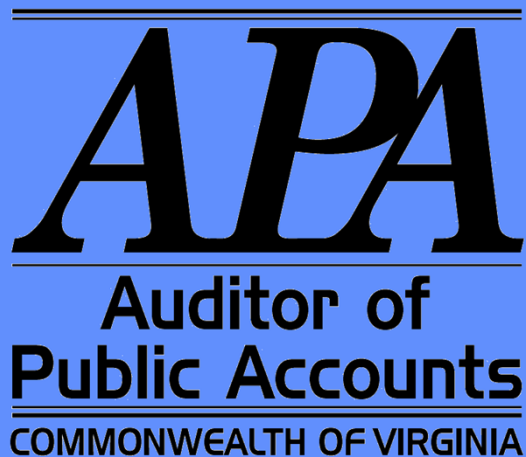


VIRGINIA PORT AUTHORITY

**REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2011**



AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Port Authority as of and for the year ended June 30, 2011, and have issued our report thereon, dated October 31, 2011. Our report on the financial statements is included in the Comprehensive Annual Financial Report issued by the Authority on November 1, 2011.

Our audit of the Virginia Port Authority for the year ended June 30, 2011, found:

- the financial statements are presented fairly, in all material respects;
- certain matters involving internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- no instances of noncompliance or other matters required to be reported under Government Auditing Standards.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS	1
INDEPENDENT AUDITOR'S REPORT	2-3
AGENCY RESPONSE	4-5
AGENCY OFFICIALS	6

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Improve IT Security Program (repeat finding)

The Virginia Port Authority (Authority) is continuing to improve its IT Security program since our last review. While the Authority's security program is still missing some components that will improve controls to safeguard mission critical and confidential data, the Authority and its IT service provider, Virginia International Terminals (VIT), contracted with an IT security firm to perform a comprehensive information security program review.

The review found that the Authority and VIT need to improve nine specific areas of concern. Due to the sensitivity and the descriptions of a security system, we do not disclose the specific weaknesses in this recommendation and in accordance with Section 2.2-3705.2 of the Code of Virginia this information is exempt under the Freedom of Information Act. However, we reviewed and the IT security firm communicated the weaknesses to management. The Authority and VIT intend to mitigate these weaknesses and are developing a detailed timeline for implementation.

We recommend that the Authority, together with VIT, implement the recommendations identified by the IT security firm. We also recommend that the Authority update its IT security program to include the data safeguard requirements of its IT service provider, VIT. The Authority should also communicate these requirements to VIT and request periodic audits of the VIT systems environment to ensure compliance.

Improve Microsoft SQL Server Security

The Authority does not manage its Microsoft SQL databases to minimize the risk of malicious or unapproved modification of data. The Authority should document and implement a baseline set of internal controls to prevent and detect malicious actions against mission critical data. Industry best practices recommend some of these controls and the others are necessary to compensate for other weaknesses in an IT environment.

Specifically, the Authority needs to improve areas of operating system and application logical access, operating system configuration, authentication, password management, and security updates. We have communicated the details of these weaknesses to management in a separate document that is exempt under the Freedom of Information Act in accordance with Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of a security system.

We recommend that the Authority dedicate the necessary resources to continue improving Microsoft SQL Server database management. At a minimum, the Authority should consider establishing controls for the weaknesses noted above or specify compensating controls for those items not mitigated. We also encourage the Authority to run freely available scanning tools to ensure compliance with best practices and timely application of the latest security updates.



Commonwealth of Virginia

Auditor of Public Accounts

Walter J. Kucharski
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

October 31, 2011

The Honorable Robert F. McDonnell
Governor of Virginia

The Honorable Charles J. Colgan
Chairman, Joint Legislative Audit
And Review Commission

Board of Commissioners
Virginia Port Authority

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited the financial statements of the business-type activities and aggregate discretely presented component unit of the **Virginia Port Authority** as of and for the year ended June 30, 2011, which collectively comprise the Authority's basic financial statements and have issued our report thereon dated October 31, 2011. Our report includes a reference to other auditors. 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. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component unit of the Authority, which were audited by other auditors and reported on separately by those auditors.

Internal Control Over Financial Reporting

Management of the Authority is responsible for establishing and maintaining effective internal control over financial reporting. In planning and performing our audit, we considered the Authority's internal control over financial reporting as a basis for designing our auditing procedures 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 over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control over financial reporting.

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.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be deficiencies, significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies in internal control over financial reporting entitled “Improve IT Security Program” and “Improve Microsoft SQL Server Security,” which are described in the section titled “Internal Control Findings and Recommendations,” that we consider to be significant deficiencies in internal control over financial reporting. 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.

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.

The Authority’s response to the findings identified in our audit is included in the section titled “Agency Response.” We did not audit the Authority’s response and, accordingly, we express no opinion on it.

Status of Prior Findings

The Authority has not taken adequate corrective action with respect to the previously reported finding “Improve IT Security Program.” Accordingly, we included this finding in the section entitled “Internal Control Findings and Recommendations.”

Report Distribution and Exit Conference

The “Independent Auditor’s Report on Internal Control over Financial Reporting and on Compliance and Other Matters” is intended solely for the information and use of the Governor and General Assembly of Virginia, Board of Commissioners, and management, and is not intended to be and should not be used by anyone, other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

We discussed this report with management at an exit conference held on November 7, 2011.

AUDITOR OF PUBLIC ACCOUNTS

DBC/alh



BOARD OF COMMISSIONERS

Michael J. Quillen, Chairman
James M. Boyd, Vice Chairman
Jennifer D. Aument
Scott R. Bergeron
Juliann J. Clemente
The Hon. William H. Fralin, Jr.
Frank E. Laughon, Jr.
John N. Pullen
Robert M. Stanton
Jeffrey D. Wassmer
Ting Xu
Manju S. Ganeriwala, *State Treasurer*

Virginia Port Authority
600 World Trade Center
Norfolk, Virginia 23510-1679
Telephone (757) 683-8000
Fax (757) 683-8500

Jerry A. Bridges
Executive Director

ISO Certified: 9001
Quality Management System -
14001 Environmental
Management System

October 31, 2011

Walter Kucharski
The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Re: Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters

Dear Mr. Kucharski:

During the normal course of the Auditor of Public Accounts Audit of the financials statements of the Virginia Port Authority as of and for the year ended June 30, 2011 you noted a certain matters involving the policy and procedures with respect to information technology and areas of weakness with respect to controls. The reportable conditions were described as follows:

Improve IT Security Program (repeat finding)

The Virginia Port Authority (Authority) is continuing to improve its IT Security program since our last review. While the Authority's security program is still missing some components that will improve controls to safeguard mission critical and confidential data, the Authority and its IT service provider, Virginia International Terminals (VIT), contracted with an IT security firm to perform a comprehensive information security program review.

The review found that the Authority and VIT need to improve nine specific areas of concern. Due to the sensitivity and the descriptions of a security system, we do not disclose the specific weaknesses in this recommendation and in accordance with Section 2.2-3705.2 of the Code of Virginia this information is exempt under the Freedom of Information Act. However, we reviewed and the IT security firm communicated the weaknesses to management. The Authority and VIT intend to mitigate these weaknesses and are developing a detailed timeline for implementation.

We recommend that the Authority, together with VIT, implement the recommendations identified by the IT security firm. We also recommend that the Authority update its IT security program to include the data safeguard requirements of its IT service provider, VIT. The Authority should also communicate these requirements to VIT and request periodic audits of the VIT systems environment to ensure compliance.

Authority Response:

The Authority and VIT have contracted with a 3rd party vendor to implement the areas of weakness noted during the comprehensive Risk Assessment conducted in 2011. The Authority also intends to include

reporting and monitoring requirements to ensure compliance by VIT with the updated policies and procedures. Full implementation is expected to take one year.

Improve Microsoft SQL Server Security

The Authority does not manage its Microsoft SQL databases to minimize the risk of malicious or unapproved modification of data. The Authority should document and implement a baseline set of internal controls to prevent and detect malicious actions against mission critical data. Industry best practices recommend some of these controls and the others are necessary to compensate for other weaknesses in an IT environment.

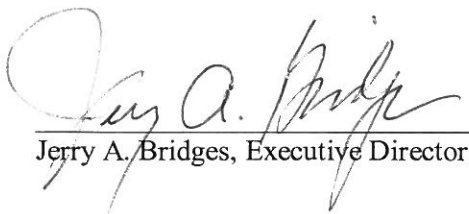
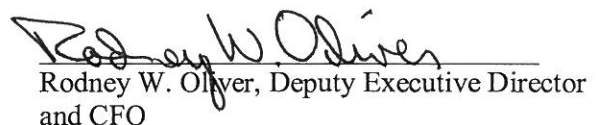
Specifically, the Authority needs to improve areas of operating system and application logical access, operating system configuration, authentication, password management, and security updates. We have communicated the details of these weaknesses to management in a separate document that is exempt under the Freedom of Information Act in accordance with Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of a security system.

We recommend that the Authority dedicate the necessary resources to continue improving Microsoft SQL Server database management. At a minimum, the Authority should consider establishing controls for the weaknesses noted above or specify compensating controls for those items not mitigated. We also encourage the Authority to run freely available scanning tools to ensure compliance with best practices and timely application of the latest security updates.

Authority Response:

The databases in question relate only to the databases on the Authority's financial accounting server. That server was originally configured by the Authority's financial accounting software support vendor. Responsibility for the configuration, security, support, and management of the SQL databases was not specifically addressed with VIT and the accounting software support vendor on the initial transition to VIT in 2006. As a result of comments from the auditors, the Authority has addressed the management of the SQL databases with VIT and the accounting software support vendor, and established clear lines of responsibilities. VIT is taking proactive measures to provide the necessary resolutions in accordance with Best Business Practices and to incorporate those measures with the management of other Authority servers and databases. Additionally, once the specific items are addressed, VIT will implement ongoing procedures and internal control monitoring mechanisms to assure that the proper security measures remain intact. In the event that implementing a specified prescriptive security measure to a given SQL Server database may adversely affect a related software application which is integrated with that database, VIT will notate those cases and report them to the Authority for further guidance. Implementation is expected to be completed within 90 days.

Sincerely,


Jerry A. Bridges, Executive Director
Rodney W. Oliver, Deputy Executive Director
and CFO

VIRGINIA PORT AUTHORITY

Norfolk, Virginia
(as of June 30, 2011)

BOARD OF COMMISSIONERS

John G. Milliken, Chairman

Deborah K. Sterns, Vice Chairman

Stephen M. Cumbie	Mark B. Goodwin
Joe B. Fleming	Allen R. Jones, Jr.
Barbara J. Fried	John Granger Macfarlane, II
Marvin S. Friedberg	Michael Jack Quillen

Thomas M. Wolf

Manju S. Ganeriwala, State Treasurer
(ex-officio member of the Board)

Jerry A. Bridges, Executive Director

Rodney W. Oliver, Treasurer to the Board

Debra McNulty, Clerk to the Board

Jodie Asbell, Deputy Clerk to the Board