

**VIRGINIA PORT AUTHORITY**

**REPORT ON AUDIT  
FOR THE YEAR ENDED  
JUNE 30, 2010**



## **AUDIT SUMMARY**

We have audited the basic financial statements of the Virginia Port Authority as of and for the year ended June 30, 2010, and have issued our report thereon, dated October 29, 2010. Our report on the financial statements is included in the Comprehensive Annual Financial Report issued by the Authority on or around November 1, 2010.

Our audit of the Virginia Port Authority for the year ended June 30, 2010 found:

- the financial statements are presented fairly, in all material respects;
- a certain matter involving an internal control finding requiring management's attention; however, we do not consider it to be a material weakness; 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 FINDING AND RECOMMENDATION	1
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	2-3
AGENCY RESPONSE	4-5
AGENCY OFFICIALS	6

## INTERNAL CONTROL FINDING AND RECOMMENDATIONS

### Improve IT Security Program

The Virginia Port Authority (Authority) has an information security program; however, it is not up to date and does not focus on a specific information security industry best practice. Without documenting and implementing a specific industry best practice and keeping it current, the Authority's Board of Commissioners (Board) significantly increases the risk that someone could either compromise or change data without authorization.

There are two predominant industry best practices that enterprises follow around the world. The first is the International Organization for Standardization's ISO27002, and the second is the COBIT Framework for IT Governance and Control by ISACA. In addition, the Commonwealth has its own set of information security standards, SEC501. We recommend that the Board select and implement one of these standards to decrease the risks mentioned above. The Authority also needs a comprehensive security program to communicate the Board's security expectations to its IT Infrastructure provider, the Virginia International Terminals (VIT). The Board should also require that VIT implement and follow an industry best practice to meet the Authority's security expectations. The Authority can verify these expectations by obtaining an independent security audit of VIT's security program and controls.



# Commonwealth of Virginia

**Walter J. Kucharski, Auditor**

**Auditor of Public Accounts  
P.O. Box 1295  
Richmond, Virginia 23218**

October 29, 2010

The Honorable Robert F. McDonnell  
Governor of Virginia

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

Board of Commissions  
Virginia Port Authority

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

We have audited the basic financial statements of the **Virginia Port Authority** (Authority) as of and for the year ended June 30, 2010, and have issued our report thereon dated October 29, 2010. 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.

### 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 opinions 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,” which are described in the section titled “Internal Control and Compliance Finding and Recommendation,” 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 finding 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.

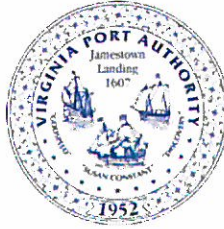
#### Report Distribution and Exit Conference

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 4, 2010.

AUDITOR OF PUBLIC ACCOUNTS

DBC/clj



#### BOARD OF COMMISSIONERS

John G. Milliken, Chairman  
Deborah K. Stearns, Vice Chairwoman  
Stephen M. Cumbie  
Joe B. Fleming  
Barbara J. Fried  
Marvin S. Friedberg  
J. Granger Macfarlane  
Mark B. Goodwin  
Allen R. Jones, Jr.  
Michael J. Quillen  
Thomas M. Wolf  
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

November 1, 2010

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, 2010 you noted a certain matter involving the internal control over financial reporting and its operation that you considered to be a reportable condition. The reportable condition was described as follows:

#### **Improve IT Security Program**

The Virginia Port Authority (Port Authority) has an information security program; however, it is not up to date and does not focus on a specific information security industry best practice. Without documenting and implementing a specific industry best practice and keeping it current, the Port Authority's Board of Commissioners (Board) significantly increases the risk that someone could either compromise or change data without authorization.

There are two predominant industry best practices that enterprises follow around the world. The first is the International Organization for Standardization's ISO27002, and the second is the COBIT Framework for IT Governance and Control by ISACA. In addition, the Commonwealth has its own set of information security standards, SEC501. We recommend that the Board select and implement one of these standards to decrease the risks mentioned above. The Authority also needs a comprehensive security program to communicate the Board's security expectations to its IT Infrastructure provider, the Virginia International Terminals (VIT). The Board should also require that VIT implement and follow an industry best practice to meet the Authority's security expectations. The Authority can verify these expectations by obtaining an independent security audit of VIT's security program and controls.



## Authority Response:

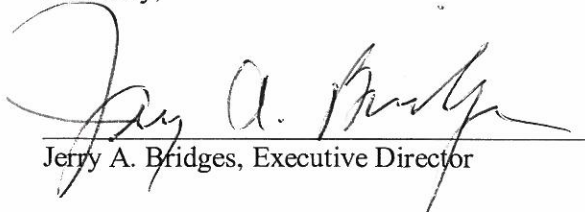
The Virginia Port Authority has a comprehensive set of information security policies and procedures that include 1) an Information Systems Security Policies and Procedures Manual (ISSP), 2) a Continuity of Operations Plan (COOP), including IT COOP, 3) a Disaster Recovery (DR) Plan, and 4) a formal Risk Assessment. The ISSP manual was last updated effective July 1, 2009. The COOP, including the IT COOP, was last updated May 31, 2010. The DR plan and formal Risk Assessment was last updated in April 2009. In addition to the formal policy manual updates, Authority staff have been provided with additional security policies throughout the year, including an August 2009 implementation and update to the Authority's password policies. We consider our IT policies and procedures to be substantially current.

The Virginia Port Authority is exempt from all aspects of the Virginia Information Technology Agency (VITA) per Chapter 874 Item 434 B of the 2010 Acts of Assembly. ("The provisions of Title 2.2 Chapter 20.1 of the Code of Virginia [establishing VITA and its powers] shall not apply to the Virginia Port Authority.") VITA is the agency that establishes the information security policies and standards for the Commonwealth. As the exemption from VITA in the Act encompasses all aspects of VITA, including their powers to set policy, standards, and procedures, the Authority is exempt from VITA mandates.

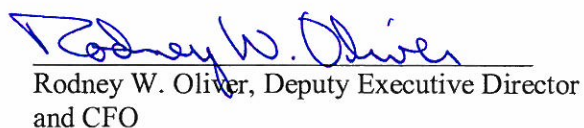
When the Authority established its information security policies and procedures in 2007, it did so with the assistance of a 3<sup>rd</sup> party, and by using as a guide the Commonwealth of Virginia (COV) section 501 standards in existence at that time. Since 2007, the Authority's policies and procedures have been updated and implemented with the COV section 501 standard as a guide, but not as a mandate. (A perfect example of that is the August 2009 update of Authority password policies from 6 characters to 8, in accordance with the August 2009 update of the COV standard, and the requirement to update the password every 90 days rather than the COV requirement of every 42 days.) The other industry best practices noted above have not been reviewed in conjunction with the Authority's established policies. However, it should be noted that those "best practices" are not worldwide mandates but rather a guide to best practices. The Authority will consider using one or more of those standards as a guide in its next formal review and update of its IT policies and procedures.

In 2007 the Authority outsourced its IT responsibilities to VIT. A contract was written outlining, among other things, the performance requirements of VIT. That contract was later enhanced in 2009 to require VIT to adhere to more specific performance requirements. During fiscal year 2010, as a good business practice (and at the request of the APA), the Authority had VIT contract with a 3<sup>rd</sup> party to conduct penetration testing for all VPA servers, networks, and systems running on VIT hardware/software. The penetration testing covered router security, firewall security, VPN security, and server security. Comments and recommendations from the 100+ page 3<sup>rd</sup> party report were reviewed and discussed with VIT and certain measures implemented by VIT to improve security. (It should be noted that the report noted no major unmitigated security risks or violations by VIT.) The Authority does concur that it needs to gain further assurance from VIT of its adoption and compliance with industry best practices and will work with VIT management to implement a plan gain such assurance.

Sincerely,



Jerry A. Bridges, Executive Director



Rodney W. Oliver, Deputy Executive Director  
and CFO



VIRGINIA PORT AUTHORITY

Norfolk, Virginia

BOARD OF COMMISSIONERS

John G. Millikan, Chairman

Deborah K. Stearns, Vice Chairwoman

Stephen M. Cumbie

Joe B. Fleming

Barbara J. Fried

Marvin S. Friedberg

Mark B. Goodwin

Allen R. Jones

J. Granger Macfarlane, II

Michael J. 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