VIRGINIA PORT AUTHORITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2008

APA

Auditor of Public Accounts

COMMONWEALTH OF VIRGINIA

AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Port Authority as of and for the year ending June 30, 2008, and have issued our report thereon, dated October 29, 2008. Our report on the financial statements is included in the Comprehensive Annual Financial Report issued by the Authority.

Our audit of the Virginia Port Authority for the year ended June 30, 2008 found:

- the financial statements are presented fairly, in all material respects;
- certain matters that we consider to be significant deficiencies in internal control; 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-

	Pages
AUDIT SUMMARY	
INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS	1-2
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	3-5
AGENCY RESPONSE	6-9
AGENCY OFFICIALS	10

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Improve Physical Access Controls

The Authority should improve its procedures for granting, changing, or removing physical access to buildings, including access to the server room housing sensitive data. Currently, the Port Police grant access to restricted areas after receiving an email request by the individual's supervisor and the building owner. The Port Police typically remove an individual's access when an employee leaves the Authority, by removing all accesses associated with the badge. The Authority has implemented a biannual review of building access by the building owner; however, evidence of this review for the server room does not exist.

As of October 15, 2008, the following individuals had access to Virginia International Terminal's Server Room: 92 police officers; 26 Technology technicians, system administrators, and other related positions; 34 non-police, non-IT individuals, including two administrative assistants a retired police officer, and a number of analysts and maintenance personnel; and four contractors; totaling 156 individuals with access to the server room. Best practices would limit the access to this room to individuals with a legitimate purpose to access the sensitive equipment, and 156 is an excessive number of individuals.

The Authority should improve procedures for granting, changing and removing physical access to employees, contractors, and other individuals requiring admission to Port facilities. Improvements on existing procedures will become increasingly important as the Authority implements use of the Federal Transportation Workers Identification Credential (TWIC) instead of Authority-issued identification badges. Beginning January 13, 2009, these cards will be the exclusive method of obtaining access to secured areas at the Ports of Virginia. Since a body external to the Authority may issue these cards, it will become critical to Port security that the addition, altering, and removal of access credentials to existing cards occur in real-time.

Further, the Authority may wish to consider alterations to the physical layout of the server room with relation to Information Systems and other employees in the long-term. The current layout does not allow for proper security of servers and other hardware infrastructure, since it does not separate the equipment from the employees' work-spaces.

Obtain Assurance over Security of Information System Infrastructure

The Authority lacks assurance over the adequacy of information system infrastructure security including the servers, networks, computer terminals, and other hardware used to store and transmit financial and other critical data vital to port operations. The Authority receives no independent verification that system security policies and processes are sufficient to control and safeguard data.

The Authority relies on its component unit, Virginia International Terminals (VIT) to provide a secure and reliable information system infrastructure to support port operations. While VIT has not had an information security failure, there is no assurance that security processes in place are sufficient to mitigate or prevent future breakdowns which may impact the Authority.

Generally, third-party organizations providing support services, like the arrangement described above, must demonstrate that they have adequate controls and safeguards when they host or process data belonging to someone else through an independent review of information security. Because VIT does not have an independent review of information system security, they cannot provide this assurance to the Authority.

The Authority should require that VIT seek out an independent third-party to audit the controls and safeguards within the current information security environment to provide assurance that those controls and safeguards are sufficient to protect the Authority's most critical data.

Improve Logical Access Controls

We reviewed the Authority's access listing, and determined that six individuals have access to both create and approve batched transactions in Commonwealth Accounting and Report System (CARS). We also determined that one individual created and approved 24 batches, and one employee created and approved one batch. These individuals have total control over the information in these batches and could have made changes including directing payments to sources other than the original documentation.

Although our review found no indication of improper transactions within these batches, failure to separate the batch entry and batch approval duties provides an opportunity for individuals to make improper vendor payments. Considering the number of users that have entry and approval access privileges; the Authority has the resources to ensure further segregation of duties by eliminating this type of access. Given that the Authority performs a monthly reconciliation that would eventually detect any inappropriate transactions; we do not consider this a material weakness in internal control.

We recommend that the Authority separate the duties of batch entry and approval when dealing with the same batch of transactions. We also recommend that the Authority review the current users that have access to CARS and determine whether such access is necessary and/or reasonable.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

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

October 29, 2008

The Honorable Timothy M. Kaine
Governor of Virginia

The Honorable M. Kirkland Cox
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 basic financial statements of the Virginia Port Authority (Authority) as of and for the year ended June 30, 2008, and have issued our report thereon dated October 29, 2008. 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 Virginia International Terminals, Inc., a component unit of the Authority, which was audited by other auditors.

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.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control over financial reporting. We consider the deficiencies entitled "Improve Physical Access Controls" and "Obtain Assurance over Security of Information System Infrastructure", which are described in the section titled "Internal Control Findings and Recommendations", to be significant deficiencies in internal control over financial reporting.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in the internal control over financial reporting that might be significant deficiencies and, accordingly, would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, we believe that none of the significant deficiencies described above is a material weakness.

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.

We noted certain matters that we reported to management of the Authority in a separate report dated August 15, 2008. Management has taken appropriate action to resolve those matters since that time.

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.

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, the 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 October 28, 2008.

AUDITOR OF PUBLIC ACCOUNTS

AWP/clj

COMMONWEALTH of VIRGINIA

BOARD OF COMMISSIONERS

John G. Milliken, Chairman
Robert C. Barclay, IV, Vice Chairman
Martin J. Barrington
Stephen M. Cumbie
Joe B. Fleming
Mark B. Goodwin
Allen R. Jones, Jr.
Michael J. Quillen
Ranjit K. Sen
Deborah K. Stearns
Thomas M. Wolf
J. Braxton Powell, *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

October 30, 2008

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

Re: Independent Auditor's Report on Internal Controls 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 financial statements of the Virginia Port Authority as of and for the year ended June 30, 2008 you noted a certain matters involving the internal control over financial reporting and its operation that you considered to be significant deficiencies. The deficiencies noted and the Authority's responses are described as follows:

Improve Physical Access Controls

The Authority should improve its procedures for granting, changing, or removing physical access to buildings, including access to the server room housing sensitive data. Currently, the Port Police grant access to restricted areas after receiving an email request by the individual's supervisor and the building owner. The Port Police typically remove an individual's access when an employee leaves the Authority, by removing all accesses associated with the badge. The Authority has implemented a biannual review of building access by the building owner; however, evidence of this review for the server room does not exist.

As of October 15, 2008, the following individuals had access to Virginia International Terminal's Server Room: 92 police officers; 26 Technology technicians, system administrators, and other related positions; 34 non-police, non-IT individuals, including two administrative assistants a retired police officer, and a number of analysts and maintenance personnel; and four contractors; totaling 156 individuals with access to the server room. Best practices would limit the access to this room to

individuals with a legitimate purpose to access the sensitive equipment, and 156 is an excessive number of individuals.

The Authority should improve procedures for granting, changing and removing physical access to employees, contractors, and other individuals requiring admission to Port facilities. Improvements on existing procedures will become increasingly important as the Authority implements use of the Federal Transportation Workers Identification Credential (TWIC) instead of Authority-issued identification badges. Beginning January 13, 2009, these cards will be the exclusive method of obtaining access to secured areas at the Ports of Virginia. Since a body external to the Authority may issue these cards, it will become critical to Port security that the addition, altering, and removal of access credentials to existing cards occur in real-time.

Further, the Authority may wish to consider alterations to the physical layout of the server room with relation to Information Systems and other employees in the long-term. The current layout does not allow for proper security of servers and other hardware infrastructure, since it does not separate the equipment from the employees' work-spaces.

Authority Response:

The Authority does have a written procedure (and a form) for granting initial physical access to buildings, including the VIT server room. However, those procedures do not extend to auditing the access list and subsequently changing or removing physical access to buildings as job responsibilities and needs change. The Authority also agrees that the number of individuals granted access to VIT's server room is excessive. Corrective action with regards to both points will be taken.

With regards to an excessive number of individuals with access to the VIT server room, the Authority does grant "full" access to all occupied spaces to VPA Port Police. Anything less would be unadvisable from a police perspective. This is similar to having a "special fire box" located in each building entrance that has full access privileges for use by the local fire department. This box is accessed by the master "fire" key by the responding fire department. No more than would we want to restrict the fire department from full access would we want to restrict the police first responders. Regarding the retired police officer, that employee was rehired as a part-time employee and, therefore, access privileges remain. The Authority will review the remaining individuals granted access as noted below and adjust access privileges accordingly.

The Authority will also address the physical layout of the server room with Virginia International Terminals to determine if a more appropriate layout would be feasible.

Obtain Assurance over Security of Information System Infrastructure

The Virginia Port Authority (Authority) lacks assurance over the adequacy of information system infrastructure security including the servers, networks, computer terminals, and other hardware used to store and transmit financial and other critical data vital to port operations. The Authority receives no independent verification that system security policies and processes are sufficient to control and safeguard data.

The Authority relies on its component unit, Virginia International Terminals (VIT) to provide a secure and reliable information system infrastructure to support port operations. While VIT has not had an

information security failure, there is no assurance that security processes in place are sufficient to mitigate or prevent future breakdowns which may impact the Authority.

Generally, third-party organizations providing support services, like the arrangement described above, must demonstrate that they have adequate controls and safeguards when they host or process data belonging to someone else through an independent review of information security. Because VIT does not have an independent review of information system security, they cannot provide this assurance to the Authority.

The Authority should require that VIT seek out an independent third-party to audit the controls and safeguards within the current information security environment to provide assurance that those controls and safeguards are sufficient to protect the Authority's most critical data.

Authority Response:

The Virginia Port Authority recognizes the need for independent third-party review of controls and safeguards of its information systems and infrastructure, and that no formal review took place during fiscal year 2008. As such, during the budget formulation process for fiscal year 2009 the Authority budgeted $15,000 for an independent third-party review. The review has not yet been initiated due to the budget shortfalls occurring at the state level, the requests for budget reductions, and the close scrutiny over new management consulting contracts. However, emphasis by the auditor demonstrates the importance of the review and, as a result; the Authority intends to hire a contractor within the next 90 days to conduct such a review.

Improve Logical Access Controls

We reviewed the Authority's access listing, and determined that six individuals have access to both create and approve batched transactions in Commonwealth Accounting and Report System (CARS). We also determined that one individual created and approved 24 batches, and one employee created and approved one batch. These individuals have total control over the information in these batches and could have made changes including direct payments to sources other than the original documentation.

Although our review found no indication of improper transactions within these batches, failure to separate the batch entry and batch approval duties provides an opportunity for individuals to make improper vendor payments. Considering the number of users that have entry and approval access privileges; the Authority has the resources to ensure further segregation of duties by eliminating this type of access. Given that the Authority performs a monthly reconciliation that would eventually detect any inappropriate transactions; we do not consider this a material weakness in internal control.

We recommend that the Authority separate the duties of batch entry and approval when dealing with the same batch of transactions. We also recommend that the Authority review the current users that have access to CARS and determine whether such access is necessary and/or reasonable.

Authority Response:

The Authority agrees with the finding that too many individuals have access to both create and approve batched transactions in CARS, and that individuals on occasion both created and approved their own batch.

As an agency authorized to maintain an independent accounting information system, the CARS system is not the primary accounting system for the Authority. The vast majority of cash receipt and payables transactions, as well as journal entries are made in the Authority's independent system. Nonetheless, strengthening controls over CARS access is a concern. The Authority has taken steps to eliminate CARS access for two individuals noted above, to change one individual from "create and approve" access to "create" access only, and another individual to "approve" access only. The changes should be effective prior to November 7, 2008.

The Authority appreciates the opportunity to respond to the auditor's comments and looks forward to working together again in the future.

Sincerely,

Jerry A. Bridges
Executive Director

Rodney W. Oliver
Director of Finance &
Treasurer to the Board

AGENCY OFFICIALS

Virginia Port Authority

Norfolk, Virginia

BOARD OF COMMISSIONERS

John G. Millikan, Chairman

Robert C. Barclay, IV Vice Chairman

Martin J. Barrington	Stephen M. Cumbie
Joe B. Fleming	Mark B. Goodwin
Allen R. Jones	Michael J. Quillen
Ranjit K. Sen	Deborah K. Stearns

Thomas M. Wolf

J. Braxton Powell, 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