2008 STATEWIDE REVIEW

OF

INFORMATION SECURITY

IN THE

COMMONWEALTH OF VIRGINIA

REPORT ON AUDIT

AS OF

DECEMBER 12, 2008

APA
Auditor of
Public Accounts
COMMONWEALTH OF VIRGINIA

Summary of Findings

The 2008 *Statewide Review of Information Security in the Commonwealth of Virginia* contains the following findings.

1) The Commonwealth of Virginia and its agencies and institutions of higher education have made significant progress in establishing and adhering to their information security programs.

2) The Commonwealth of Virginia is continually updating its information security policies and standards to meet the needs of the Commonwealth and the requirements of industry best practices.

3) The Commonwealth of Virginia communicates information security policies, standards, and guidelines to agencies and institutions of higher education through several channels, including, monthly information security officers' meetings, new information security officer orientation, e-mail communication, and on-line review and comment forums.

4) Smaller agencies continue not to have adequate resources or expertise to establish an information security program. The Commonwealth has hired two full-time information security experts to assist small to medium-sized agencies establish information security programs; however, they have not had the time to address most the agencies' needs.

This report contains no recommendations. Appendix B includes a summary of recommendations previously given to agencies and institutions of higher education for improving their information security programs since our last statewide review of information security in December 2006.

-TABLE OF CONTENTS-

Introduction

This report contains the results of our follow-up to our *Statewide Review of Information Security in the Commonwealth of Virginia* report issued in December 2006. In addition to evaluating agencies' progress in establishing adequate information security programs, the Office also evaluated the adequacy of the agency's implementation of the programs. The last section of this report and the appendices include a detailed analysis of the progress the agencies have made in completing their programs. We conducted our review in accordance with the standards for performance audits set forth in Government Auditing Standards, issued by the Comptroller General of the United States.

Objectives

Our audit work had four objectives.

1) Determine whether agencies and institutions of higher education have adequately established and documented their information security programs.
2) Determine whether agencies and institutions of higher education have adequately operationalized and adhered to their information security programs.
3) Analyze the progress made by agencies and institutions of higher education since our last statewide information security report.
4) Determine if the Commonwealth's information security strategies continue to follow best practices.

Scope

The Office conducted field work for this report between March 2007 and November 2008 as part of our agency or institution of higher education regularly scheduled audit. During the period, we reviewed 74 of the 104 agencies and institutions of higher education included in our previous report, and plan to review the remaining 30 agencies during our audits next year. Most of the excluded agencies have less than 100 staff, and our preliminary review continues to show that these smaller agencies do not have adequate resources or expertise to establish an information security program. Although the Commonwealth has hired two full-time information security experts to assist small to medium-sized agencies establish information security programs, they have not had the time to address most agencies' needs.

Methodology

Our review consisted of two parts. The first part determined whether the agency had established and documented an information security program based on 11 information security criteria. This part of the review used the same review criteria and process followed in our December 2006 study.

Essential Security Program Components

1. A business impact analysis
2. A risk assessment
3. A continuity of operations plan
4. A disaster recovery plan
5. An organizational structure that includes the assignment of an Information Security Officer
6. A formal training program
7. Policies and procedures for approving logical access
8. Process requiring user authentication for access to all systems and management approval of any exceptions after having evaluated the risks of those exceptions
9. Policies and procedures regarding password controls
10. Appropriate physical safeguards in place to protect all the critical and sensitive assets against unauthorized access and documentation of who approves these controls
11. Active monitoring of their systems, applications, and databases

We rated each agency program as “No”, “Inadequate”, or “Adequate” based on the following criteria. Fundamental to any security program are the following four items from the *Essential Security Program Components* list above. Appendix A contains the details of the rating for each agency.

1. A business impact analysis
2. A risk assessment
3. A continuity of operations plan
4. A disaster recovery plan

These documents serve as the foundation for the security programs and any inadequacies within these processes and documents weakens the entire program. Without sufficiently documenting and performing these processes, no agency or institution of higher education can complete the remaining items of the *Essential Security Program Components* listed above.

No Information Security Program Criteria

The agency or institution did not have any of the basic documents required to perform a security assessment.

Inadequate Information Security Program Criteria

The agency had begun the process of evaluating their state of security and had at least one of the four fundamental documents; therefore, they had an inadequate information security program.

Adequate Information Security Program Criteria

The agency had an adequate security program, since they had performed a security analysis that includes documentation of all *Essential Security Program*

Components. The full security analysis must include completion of the four fundamental documents, and have additional security controls needed for an adequate security program.

The second part of the review tested an agency's information security program to determine if it followed the established processes and documents of the agency's program. We rated each agency and institution of higher education as to its operationalization and adherence to its information security program as "Inadequate" or "Adequate."

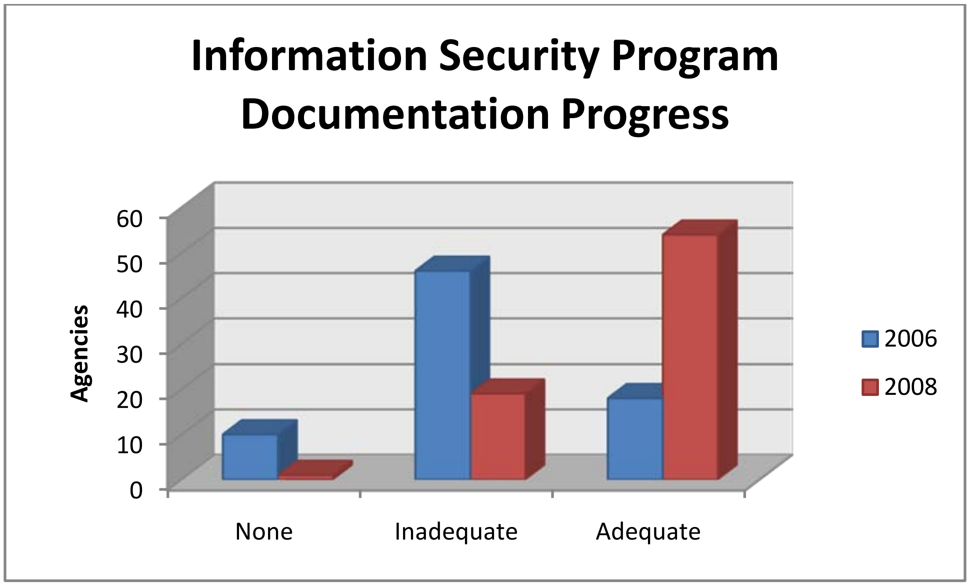
Adequate found that the agency was following and periodically updating and refining its security program. Inadequate found agencies were not performing, updating or testing significant portions of the agency's information security program.

Information Security Progress Report

In general, agencies and institutions of higher education in the Commonwealth of Virginia have significantly improved their information security programs since our last review in December 2006. Of the 74 agencies and institutions of higher education included in this review, we found six (6) had moved from No program to Inadequate and 36 more agencies and institutions of higher education had become Adequate. Overall, of the 74 agencies and institutions of higher education, there are 73 percent with Adequate programs, 26 percent with Inadequate and only one percent with No programs.

Information Security Program Documentation Progress

The following figure illustrates the progress made by the Commonwealth's agencies and institutions of higher education in documenting and establishing their information security programs.



	2006		2008	
	Agencies	**%**	**Agencies**	**%**
None	10	14%	1	1%
Inadequate	46	62%	19	26%
Adequate	18	24%	54	73%

Figure 1. *Agency information security program documentation progress.*

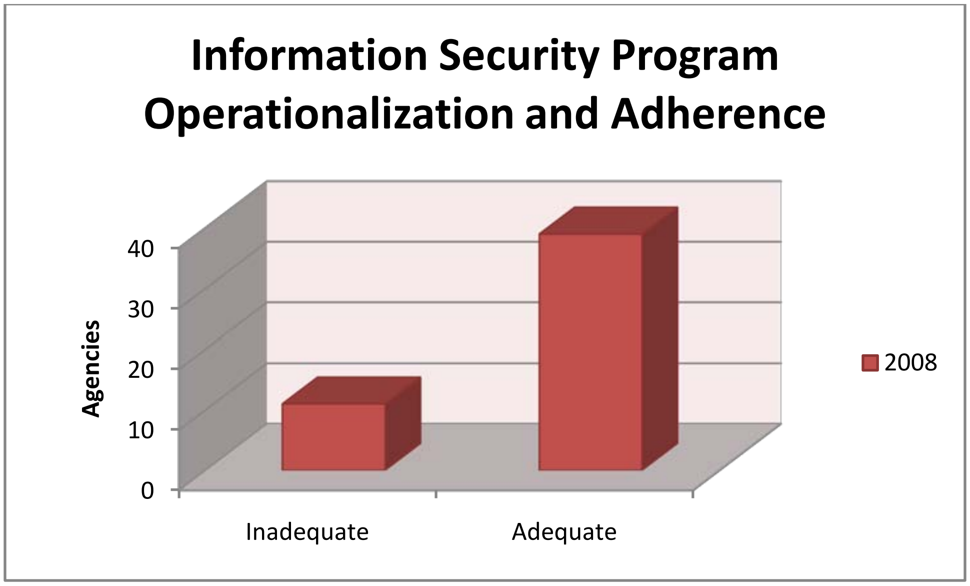
The graph and table show that only one of the 74 agencies in this study as rated as having no information security program in 2008, versus ten agencies in 2006. Similarly, we noticed an improvement of inadequate information security programs dropping from 46 agencies to 19 agencies between 2006 and 2008. Adequate programs increased from 18 agencies to 54 agencies between 2006 and 2008. The next section will discuss whether the agencies and institutions of higher education with established and documented programs follow, update, and test their information security programs.

Information Security Program Operationalization and Adherence

We also evaluated how agencies and institutions of higher education with adequate information security programs follow their established programs. Out of the 54 agencies with adequate programs, we evaluated 50 agencies. We will evaluate the remaining four agencies, Department of Military Affairs, Frontier Culture Museum of Virginia, Virginia Institute of Marine Science, and Virginia Museum of Fine Arts, during their audits next year.

Using the same 11 *Essential Security Program Components* described above, we evaluated how each agency operationalized and adhered to their information security program based on the Commonwealth's information security standard and industry best practices. We have included the detailed evaluation criteria in Appendix C of this report.

While we did not extensively evaluate agencies and institutions of higher education adherence to their information security programs in our previous report in 2006, we found in 2008 that 35 out of the 50 agencies and institutions of higher education properly follow their documented information security programs. The following graph show how agencies and institutions of higher education operationalize and adhere to their information security program.



	2008	
	Agencies	**%**
Inadequate	11	22%
Adequate	39	78%

Figure 2*. Agency information security program operationalization and adherence.*

In our analysis, we found that many of the 11 agencies that were rated as inadequate specifically need to improve updating and testing of contingency plans, including risk assessment, business impact analysis, continuity of operations plans, and disaster recovery plans, and continue security awareness training.

Contingency Plans

We found that seven, or 14 percent, out of the 50 agencies and institutions of higher education had not adequately developed, updated, and tested their continuity of operations plans, and seven, or 14 percent, out of the 50 agencies and institutions of higher education had not adequately implemented their disaster recovery plans. Some of the primary reasons for inadequate contingency plans were outdated or untested plans, and inconsistencies between the plans.

As discussed earlier in this report, four of the most fundamental parts of an information security program are the risk assessment, business impact analysis, continuity of operations plan, and the disaster recovery plan. These four parts are highly dependent on each other. An agency or institution of higher education cannot develop an adequate continuity of operations plan or disaster recovery plan without having assessed its risks in a risk assessment, or identified its business functions and impacts in a business impact analysis. In other words, the risk assessment and business impact analysis are prerequisites of the continuity of operations plan and the disaster recovery plan.

In our review, we tested whether agencies and institutions of higher education have developed, updated, and tested their contingency plans according to the Commonwealth's security standard. Of the institutions in the review, four institutions of higher education have exemptions from the Commonwealth's security standard; College of William and Mary, University of Virginia, Virginia Commonwealth University, and Virginia Polytechnic Institute and State University. In these four instances, we tested these institution's operationalization and adherence against industry best practices. Appendix C, sections C, D, E, and F contains the specific test criteria for contingency plans.

Security Awareness Program

We found that eight, or 16 percent, out of the 50 agencies and institutions of higher education had not adequately implemented their security awareness program. The primary reasons for inadequate security awareness training were the failure of some agencies and institutions of higher education to give training to employees and record attendance.

A security awareness training program should include position specific training. In other words, training for system administrators should contain material specific for their environment, compared to general user training. Also, Commonwealth agencies and institutions of higher education are required to keep records that employees received security awareness training.

Information Security and the Commonwealth

Previous Report's Recommendations

Our Office made four recommendations in our information security report issued in 2006. As part of our follow-up review, we have determined that all four recommendations have been resolved. The following paragraphs discuss the resolutions to the recommendations, followed by current strategies for information security in the Commonwealth.

> Previous Report's Recommendation #1
>
> We recommend that VITA develop a plan to communicate infrastructure information and standards to agencies that VITA supports. Additionally, VITA should provide assistance and expertise to agencies as they develop their information security programs. VITA should also assume responsibility for ensuring that the infrastructure meets the agency's needs and mitigate threats and vulnerabilities through Northrop Grumman's standards.

Virginia Information Technologies Agency (VITA) addressed this recommendation by having monthly Information Security Officer Advisory Group (ISOAG) meetings. These meetings allowed agency information security officers to discuss current information security issues facing the Commonwealth and propose and participate in the development of upcoming changes to the Commonwealth's policy, standard, and guidelines. In addition, VITA conducts several orientation classes throughout the year for newly appointed agency information security officers. VITA has added several *Information Security Guidelines* to help agencies develop comprehensive information security programs.

Previous Report's Recommendation #2

The General Assembly may wish to consider granting the CIO authority over the other branches of government's information security programs. In addition, agencies and institutions need to develop a mutual comprehensive information security program with VITA that provides adequate comprehensive security to protect information in the Commonwealth.

The 2007 General Assembly enacted legislation that changed the Code of Virginia and made the Commonwealth's CIO have overall authority for information security programs in the all branches of government.

Previous Report's Recommendation #3

The CIO and ITIB should consider supplementing the Commonwealth's SEC 501 standard with the additional processes identified in this report.

The Commonwealth's CIO and the Information Technology Investment Board (ITIB) approved for incorporation in the Commonwealth's standard the additional industry best practice processes.

Previous Report's Recommendation #4

In order to create a proper information security plan, agencies require sufficient resources with appropriate expertise to develop such plan. Using a centralized entity, such as VITA, to help with creating and maintaining an information security plan allows the Commonwealth to leverage its cost for resources with information security expertise to assist agencies, especially small to medium-sized agencies, to perform the proper security analysis and develop an adequate information security plan.

The Department of Accounts received funding to employ two full-time information security experts, who started in July, 2008. These individuals are currently establishing a work plan to help smaller-sized agencies in developing information security programs.

Information Security Strategies in the Commonwealth

The Commonwealth has implemented several information security strategies to ensure, to the largest extent possible, that its data is safe, accurate, and available. We will discuss the following strategies in this section.

1. The Commonwealth's Information Security Policies, Standards, and Guidelines
2. Executive Order 43
3. Additional duties of the CIO relating to security of government information
4. Information Security Program Oversight

The Commonwealth's Information Security Policies, Standards, and Guidelines

Several revisions of the Commonwealth's Information Technology Security Policy and Information Technology Security Standard have occurred since our last review. In addition, VITA has published new Information Security Guidelines to aid agencies in documenting and implementing their information security programs. The Commonwealth's Chief Information Security Officer (CISO) has responsibility for directing the development of policies, procedures, and standards for assessing security risks; determining the appropriate security measures; and performing security audits of government electronic information.

While certain institutions of higher education, specifically the College of William and Mary, University of Virginia, Virginia Commonwealth University, and Virginia Polytechnic Institute and State University, are exempt from the Commonwealth's information security policies and standards, they must implement information security programs that provide the same, or better, protection for their data. Three of the four institutions have decided to use a best practice known as ISO/IEC 27002:2005, which is an international code of practice for information security, and it is the same code of practice the Commonwealth uses to develop its policies and standards. The fourth institution chose to adopt the Commonwealth's information security policies and standards.

Since our December 2006 report of Information Security in the Commonwealth of Virginia, the policies, standards, and guidelines have continued to evolve to align with industry best practices.

Information Technology Security Policy (SEC500-02)

The Commonwealth's Information Technology Security Policy defines the minimum information security program for agencies in the executive, judicial and legislative branches of government. This policy establishes a framework for an information security program to protect the Commonwealth's systems and data from credible threats, whether internal or external, deliberate or accidental.

We found that VITA is updating the policy to meet the information security needs of the Commonwealth. The current fifth revision of the policy became effective July 17, 2008, and agencies have to comply with this policy as of January 1, 2009. However, academic and research systems previously exempted from the policy have a compliance date of July 1, 2009.

Information Technology Security Standard (SEC501-01)

The Commonwealth's Information Technology Security Standard defines the minimum requirements for each agency's information security program in the executive, judicial and legislative branches of government. The standard establishes a baseline for information security controls which will provide protection of the Commonwealth's systems and data.

We found VITA is keeping the standard updated to meet the information security needs of the Commonwealth. The current fourth revision of the standard became effective July 24, 2008, and agencies have to comply with this standard as of January 1, 2009. However, academic and research systems previously exempted from the standard have a compliance date of July 1, 2009.

The fourth and latest revision of the standard includes several changes and additional language, and below we provide the four significant changes and additions.

1) Data Breach Notification – The standard significantly expands the responsibilities and duties of agencies and institutions by incorporating the Data Breach Notification law in Section 18.2-186.6 of the Code of Virginia, passed by the 2008 General Assembly.
2) Email Communications – A section clarified user responsibilities and requirements when sending sensitive data in email.
3) Application Security – A section now covers security practices in developing and deploying Commonwealth applications.
4) Password Management – Several additions include password complexity, password requirements for PDAs and smart phones, and screen saver passwords.

Information Technology Security Audit Standard (SEC502-00)

The Commonwealth's Information Technology Security Audit Standard provides guidance on the coordination of information security audits at agencies and institutions of higher education, thereby eliminating any duplication of effort. Each agency has responsibility for developing and submitting an information security audit plan annually to the CISO.

Information Security Guidelines

Information Security Guidelines provide guidance to agencies and institutions of higher education on how to implement the Commonwealth's information security policies and standards. The following guidelines are available at VITA's website, http://www.vita.virginia.gov/security.

- Internet Privacy Guidelines (SEC2001-02)
- IT Contingency Planning Guideline (SEC508-00)
- IT Data Protection Guideline (SEC507-00)
- IT Logical Access Control Guideline (SEC509-00)
- IT Personnel Security Guideline (SEC513-00)
- IT Risk Management Guideline (SEC506-01)
- IT Security Audit Guideline (SEC512-00)
- IT Security Threat Management Guideline (SEC510-00)
- IT Systems Security Guideline (SEC515-00)

Executive Order 43

Governor Kaine issued Executive Order 43 on January 9th, 2007, entitled "Protecting the Security of Sensitive Individual Information in Executive Branch Operations." The order directs the Secretary of Technology to annually report agencies' information security compliance efforts to the Governor by October 15.

Additional Duties of the CIO Relating to Security of Government Information

The 2006 General Assembly added paragraph "C" to Section 2.2-2009 of the Code of Virginia, which directs the CIO to report those agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats to the Governor and the General Assembly by December 2008, and annually thereafter. Upon review of the results, the Information Technology Investment Board may take action to suspend or limit technology investments spending pending acceptable corrective actions.

Information Security Program Oversight

The oversight of information security in an organization as large and complex as the Commonwealth is always a challenge. The Commonwealth is leveraging this risk by transitioning agencies to a highly secured data center run by the IT Infrastructure Partnership with Northrop Grumman Corporation.

While institutions of higher education are exempt from the IT Infrastructure Partnership, agencies in the executive branch must undergo transition. Transitioning agency servers to the data center will centralize monitoring and maintenance, and provide the Commonwealth with greater security and efficiencies in protecting its data. However, there have been delays in the transition of some data centers from agencies to the new central data center. During this delay, our office is comparing the security controls at the local data centers to those available at the Commonwealth's data center. As a result, our office will report any information security deficiencies or inefficiencies resulting from operating a data center locally at an agency.

In addition to the information security reviews performed by this office, IT Infrastructure Partnership and agency information security officers are providing information security program oversight, and the following paragraphs provide a brief description of their responsibilities.

IT Infrastructure Partnership

Since our last review, the Commonwealth has progressed in transitioning its IT infrastructure, including network components and servers, from agencies in the Executive branch to the IT Infrastructure Partnership. As this transition period is nearing its end, clear information security responsibilities of the Partnership and the agencies are solidifying.

While the new data center offers agencies a standardized security baseline and equipment and data redundancy, the proper oversight of how security is implemented and transitioned is very important. VITA is managing the IT Infrastructure Partnership, which will provide Executive branch agencies computer infrastructure services through a contract with the Northrop Grumman Corporation. Deloitte & Touche, LLP audits the information security controls at the infrastructure level (servers, laptops, desktops, firewalls, etc), and annually issues an IT Infrastructure audit report to VITA, the Auditor of Public Accounts, and the affected agencies.

Auditor of Public Accounts

The Auditor of Public Accounts audits agencies and institutions of higher education in the Executive and Judicial branches of Government. The office has a dedicated information systems security specialty team that performs security audits throughout the year. All information security findings go to the agencies and public through the audit reports.

Agency Information Security Officer

Each agency and institution of higher education designates an Information Security Officer (ISO), who develops, establishes, maintains, and reviews the organization's information security program. Other duties include developing and maintaining an IT security awareness training program, implementing and maintaining the appropriate balance of protective and corrective controls for agency systems commensurate with data sensitivity, risk and systems criticality.

Conclusion

The Commonwealth has made significant improvements in securing confidential and mission critical data. While information security programs can never ensure 100 percent protection of data, the Commonwealth and its agencies and institutions of higher education have established comprehensive information security policies, standards, procedures, and guidelines that align with industry best practices and help reduce occurrences of data breach, corrupt data, and unavailable data.

Comparing the results of this study with the study reported by our office in December 2006, we can see that agencies have made significant improvements in establishing and documenting their information security programs. In 2006, we reported that 18 agencies, or 20 percent, of the 104 agencies and institutions of higher education reviewed had established information security programs. This year, we compared the progress of 74 of those agencies, and found that 54 agencies, or 73 percent, have established information security programs.

In addition, for those agencies and institutions of higher education with established and documented information security programs, we studied how the agencies and institutions of higher education operationalize and adhere to their programs. Out of the 50 agencies with established information security programs, we found that 38 agencies (76 percent) adequately follow the policies and procedures of their programs.

The Commonwealth implemented the four recommendations in our December 2006 report. The Department of Accounts has hired two information security professionals to provide expertise to small- to medium-sized agencies and they are currently establishing a work plan to assist these agencies in establishing information security programs

Commonwealth of Virginia

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

Walter J. Kucharski, Auditor

December 12, 2008

The Honorable Timothy M. Kaine
Governor of Virginia
State Capital
Richmond, Virginia

The Honorable M. Kirkland Cox
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

We have audited 74 agencies in the Commonwealth and are pleased to submit our report entitled **2008 Statewide Review of Information Security in the Commonwealth of Virginia**. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Exit Conference and Report Distribution

We discussed this report with the Commonwealth's Chief Information Officer (CIO) and the Secretary of Technology on December 12, 2008. The Commonwealth's Chief Information Officer and Secretary of Technology's responses have been included at the end of this report.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

AUDITOR OF PUBLIC ACCOUNTS

GGG/clj

COMMONWEALTH of VIRGINIA

Office of the Governor

Aneesh P. Chopra
Secretary of Technology

December 11, 2008

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

Dear Mr. Kucharski:

Thank you for the opportunity to review and respond to your 2008 Statewide Review of Information Security in the Commonwealth of Virginia.

Firstly, I want to thank you for your diligence in evaluating our agencies and thoroughness with which you have established benchmarks for us to surpass. Like you have noted, we are very pleased with the dramatic improvement in agencies designated "adequate" in the past two years. We also recognize the continued challenges faced by our smaller agencies that lack staff expertise in this critical area. We fully expect the Commonwealth's Information Security Officer will address their needs with the recent staff additions. You can rest assured that I will direct the needed resources from my office to fully support that effort.

In general, we agree with your findings and applaud the hard work at the various levels of government that have contributed to the progress in strengthening our Information Security posture. Thank you and your staff for your work on this report.

Sincerely,

Aneesh P. Chopra

COMMONWEALTH of VIRGINIA

Lemuel C. Stewart, Jr.
Chief Information Officer
Email: cio@vita.virginia.gov

Virginia Information Technologies Agency
11751 Meadowville Lane
Chester, Virginia 23836-6315
(804) 416-6100

TDD VOICE -TEL. NO.
711

December 8, 2008

Mr. Walter J. Kucharski
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218

Dear Mr. Kucharski:

Thank you for the opportunity to review and respond to the Auditor of Public Accounts' 2008 Statewide Review of Information Security in the Commonwealth of Virginia. The review highlights many of the challenges the Commonwealth has addressed and will continue to address to enhance the security of Commonwealth information.

While recognizing that strengthening the information security posture of the Commonwealth is a journey without end, we agree and appreciate the conclusion of the report that the Commonwealth has made significant improvements in securing sensitive data. We particularly look forward to the information security benefits that will be achieved when the information technology infrastructure for the Executive Branch agencies, excluding higher education, are transitioned to the Commonwealth Enterprise Solutions Center. As always, we appreciate the professionalism of your staff.

Sincerely,

Lemuel C Stewart Jr

Lemuel C. Stewart, Jr.

c: The Honorable Aneesh P. Chopra, Secretary of Technology
Judy G. Napier, Deputy Secretary of Technology
Members, Information Technology Investment Board

Appendix A – 2008 Information Security Program Ratings

This appendix contains the individual agency and institutions of higher education information security program ratings for 2008. The first rating column, "**2006 Program Documentation**," contains the rating the agency or institution of higher education received in the 2006 Statewide Review of Information Security in the Commonwealth of Virginia report.

The second rating column, "**2008 Program Documentation**," contains the follow-up ratings for this report. This column rates whether the agency or institution of higher education has documented and established an information security program.

The third rating column, "**2008 Program Operalization and Adherence**," contains the ratings the agency or institution of higher education has received for operationalizing and following its information security program. We have rated certain agencies as "INT*," which means that we did not review how the agency operationalized and follows its program due to the agency having inadequate documentation to determine what its plan is. Also, note that four of the agencies rated as "INT*", Department of Military Affairs, Frontier Culture Museum of Virginia, Virginia Institute of Marine Science, and Virginia Museum of Fine Arts, do have adequate information security program documentation, however, we will evaluate their operalization and adherence during upcoming audits.

2006 and 2008 Program Documentation Legend	
N	No Program
I	Inadequate Program
A	Adequate Program

2008 Program Operationalization and Adherence Legend	
INT*	Implementation Not Tested
I	Inadequate Implementation
A	Adequate Implementation

Agency Name	Staff†	2006 Program Documentation	2008 Program Documentation	2008 Program Operationalization and Adherence
Attorney General and Department of Law	357	I	A	A
Board of Accountancy	13	I	A	A
Board of Bar Examiners	8	N	N	INT*
Christopher Newport University	1,259	A	A	A
College of William and Mary	2,323	I	A	A
Department of Accounts	143	A	A	I

Agency Name	Staff†	2006 Program Documentation	2008 Program Documentation	2008 Program Operationalization and Adherence
Department of Agriculture and Consumer Services	711	N	A	A
Department of Alcoholic Beverage Control	6,032	I	A	A
Department of Business Assistance	57	I	I	INT*
Department of Conservation and Recreation	1,343	I	A	I
Department of Correctional Education	889	I	I	INT*
Department of Corrections	12,983	A	A	A
Department of Education	484	I	I	INT*
Department of Emergency Management	206	I	A	I
Department of Environmental Quality	1,035	I	A	A
Department of Fire Programs	129	I	I	INT*
Department of Forensic Science	376	N	A	A
Department of Game and Inland Fisheries	600	I	I	INT*
Department of General Services	734	A	A	A
Department of Health	4,884	I	A	I
Department of Health Professions	273	A	A	A
Department of Historic Resources	56	I	I	INT*
Department of Juvenile Justice	3,013	I	A	I
Department of Labor and Industry	200	I	A	A
Department of Medical Assistance Services	531	I	A	A
Department of Mental Health, Mental Retardation and Substance Abuse Svs	10,923	I	A	I
Department of Military Affairs	691	I	A	INT*
Department of Mines, Minerals and Energy	250	I	A	A
Department of Minority Business Enterprises	57	N	I	INT*
Department of Motor Vehicles	2,683	I	A	A
Department of Professional and Occupational Regulation	221	I	I	INT*
Department of Rehabilitative Services	1,008	A	A	A
Department of Social Services	1,998	I	A	A
Department of State Police	3,234	I	A	A
Department of Taxation	1,423	A	A	A
Department of the Treasury	131	I	I	INT*

Agency Name	Staff†	2006 Program Documentation	2008 Program Documentation	2008 Program Operationalization and Adherence
Department of Transportation	10,180	I	A	A
Department of Veterans Services	282	N	I	INT*
Frontier Culture Museum of Virginia	93	N	A	INT*
George Mason University	9,028	I	A	A
Gunston Hall	19	N	I	INT*
Indigent Defense Commission	NA	N	I	INT*
Innovative Technology Authority / Center for Innovative Technology	NA	A	A	A
James Madison University	3,426	A	A	A
Jamestown-Yorktown Foundation and Jamestown 2007	617	I	I	INT*
Longwood University	1,085	I	A	I
Marine Resources Commission	171	I	A	I
Norfolk State University	1,170	I	A	A
Old Dominion University	3,693	I	A	A
Radford University	1,377	I	A	A
Richard Bland College	141	I	A	A
Science Museum of Virginia	186	I	I	INT*
State Corporation Commission	697	N	I	INT*
State Lottery Department	301	I	A	I
Supreme Court of Virginia	221	I	I	INT*
University of Mary Washington	1,307	I	A	A
University of Virginia	8,150	A	A	A
University of Virginia – Medical Center	6,073	I	A	A
Virginia College Savings Plan	54	A	A	A
Virginia Commonwealth University	8,624	A	A	A
Virginia Community College System	8,819	A	A	A
Virginia Economic Development Partnership	123	I	A	A
Virginia Employment Commission	1,385	I	A	A
Virginia Information Technologies Agency	446	A	A	A
Virginia Institute of Marine Science	437	I	A	INT*
Virginia Military Institute	575	A	A	I

Agency Name	Staff†	2006 Program Documentation	2008 Program Documentation	2008 Program Operationalization and Adherence
Virginia Museum of Fine Arts	495	I	A	INT*
Virginia Museum of Natural History	63	I	I	INT*
Virginia Polytechnic Institute and State University	9,860	A	A	A
Virginia Port Authority	180	A	A	I
Virginia Retirement System	319	A	A	A
Virginia State Bar	114	N	I	INT*
Virginia State University	885	I	A	A
Virginia Workers' Compensation Commission	241	I	I	INT*

Notes

***** INT, or Implementation Not Tested, means that we evaluated the agency's information security program documentation and found it adequate; however, we did not review its implementation. Or we found the agency's information security program documentation inadequate, and we did not continue to test how the agency operationalized or adhered to its program. We rated four agencies, Department of Military Affairs, Frontier Culture Museum of Virginia, Virginia Institute of Marine Science, and Virginia Museum of Fine Arts, as having a documented information security program, however, our office has not tested how these agencies operationalize and adhere to their programs and will test the plan in future audits.

† Staff counts use the 2008 salary and wage state employee counts as reported by the Commonwealth Datapoint website, found at: http://datapoint.apa.virginia.gov.

Appendix B – Information Security Program Findings Summary

This appendix is a summary of the information security program findings that we have issued to agencies and institutions of higher education through our normal audit process, with the exception of five agencies asterisked below. For those five, we have discussed the findings with the agencies, and we plan to issue the report in the near future. The audit reports for all agencies and institutions of higher education mentioned in this report are available from our website, at http://www.apa.virginia.gov/reports.cfm.

Each of the agencies and institutions of higher education received one or more findings in the five general categories of an information security program shown with an "I" (Inadequate). The severity of the findings can affect the overall rating we give individual agencies and institutions of higher education, however, some agencies and institutions of higher education can have an ADEQUATE program with findings.

Agency Name	Contingency Plans	Information Security Officer	Security Awareness Training	Physical And Logical Access	Monitoring
Board of Bar Examiners	I		I		
Department of Accounts	I			I	I
Department of Business Assistance	I		I	I	I
Department of Conservation and Recreation	I		I	I	I
Department of Correctional Education*				I	
Department of Education				I	
Department of Emergency Management	I		I		
Department of Fire Programs	I		I	I	
Department of Game and Inland Fisheries	I			I	
Department of Health	I		I	I	
Department of Historic Resources	I	I	I	I	I
Department of Juvenile Justice*				I	
Department of Mental Health, Mental Retardation and Substance Abuse Svs	I		I		
Department of Minority Business Enterprises	I			I	
Department of Professional and Occupational Regulation*				I	I
Department of the Treasury	I		I		
Department of Veterans Services	I			I	
Gunston Hall	I	I	I	I	

Agency Name	Contingency Plans	Information Security Officer	Security Awareness Training	Physical And Logical Access	Monitoring
Indigent Defense Commission	I		I	I	
Jamestown-Yorktown Foundation and Jamestown 2007	I				
Longwood University	I		I	I	
Marine Resources Commission*	I		I	I	
Science Museum of Virginia	I		I	I	
State Corporation Commission	I		I	I	
State Lottery Department	I				
Supreme Court of Virginia	I				
Virginia Community College System				I	
Virginia Institute of Marine Science*	I			I	
Virginia Military Institute				I	
Virginia Museum of Natural History			I		
Virginia Port Authority				I	
Virginia State Bar	I	I	I	I	
Virginia Workers’ Compensation Commission	I		I		

Appendix C – Information Security Program Evaluation Criteria for Operalization and Adherence

This appendix contains the criteria we used to evaluate whether an agency adequately operationalized and adhered to its information security program. These criteria use the Commonwealth's information security policy and standard, and industry best practices.

A. Information Security Officer
a. Determine if the ISO's job description includes the roles and responsibilities as identified in ITRM Policy SEC500-02 and ITRM Standard SEC501-01. b. Determine if the ISO's reporting relationship within the Agency is at a level high enough to ensure independence.
B. Security Awareness Training Program
a. Determine if general, position-specific, and technical training is provided. b. Determine if acknowledgement forms were signed for new staff and refresher training.
C. Risk Assessment (RA)
a. Determine if critical and sensitive IT systems are identified. b. Determine if the potential vulnerabilities, threats and the probability that the threat will occur are documented. c. Determine if mitigation procedures are identified for potential risks and threats. Determine if the RA has been updated within the last 3 years or earlier if warranted.
D. Business Impact Analysis (BIA)
a. Determine if essential business functions, and the IT systems and data that support those functions, are identified. b. Determine if maximum tolerable downtimes are documented.
E. Continuity of Operations Plan (COOP)
a. Determine if plans to operate essential business functions until normal operations can be restored are documented and include all processes. b. Determine if recovery requirements for IT systems and data needed to support essential business functions (based on BIA and RA) are documented. c. Determine if personnel contact information and incident notification procedures are documented. d. Determine if the COOP is tested annually for adequacy and effectiveness.
F. Disaster Recovery Plan (DRP)
a. Determine if the steps necessary to restore essential business functions that support Agency mission requirements (based on BIA and RA) are documented. b. Determine if the Disaster Recovery Plan has been tested, and if so, when was the last test performed? c. Determine if all IT Disaster Recovery team members are trained as part of the Agency's IT security training program. d. Determine is backup media is securely stored off-site. e. Review backup logs to determine that backup jobs are verified and successfully completed. f. Review how backup media is shipped and stored off-site. Does the Agency's policies direct the appropriate actions (or require a third party to take the appropriate actions) to protect backup media while in transit and storage? Sample any manifests or logs.

G. Logical Access

a. Determine that the Agency complies with the following Policies and Procedures:
   - i. Grant access to IT systems and data based on principle of least privilege.
   - ii. Establish accounts only after proper authorization and approval by the System Owner.
   - iii. Review sensitive IT system user accounts annually and periodically for other IT systems

b. Determine if account request forms were authorized in accordance with agency policy.

c. Determine if logical access was removed or changed appropriately for terminated, promoted or reassigned staff in a timely manner.

H. Authentication

a. Determine if users are required to be authenticated to all systems.

b. Password Management

c. Determine if passwords meet requirements established in the Agency’s or Institution of Higher Education’s policies and procedures.

d. Determine if the Agency enforces password controls.

I. Physical Security of mission critical and sensitive IT systems

a. Determine that the Agency complies with the following Policies and Procedures:
   - i. Grant physical access to essential or sensitive computer hardware, wiring, displays and networks by the principle of least privilege.
   - ii. Establish access only after proper authorization and approval by the System Owner.
   - iii. Review physical access to mission critical and sensitive IT systems annually.

b. Determine who has physical access and if it’s appropriate.

c. Determine if the approval process for physical access was followed.

d. Determine if physical access was removed or changed for terminated, promoted, or reassigned staff in a timely matter.

J. Monitoring

a. Determine if the agency is monitoring their systems according to their policies and that those policies are reasonable.