2010 STATE OF INFORMATION SECURITY

IN THE

COMMONWEALTH OF VIRGINIA

AS OF OCTOBER 31, 2010

APA
Auditor of
Public Accounts
COMMONWEALTH OF VIRGINIA

Executive Summary

The purpose of the *2010 State of Information Security in the Commonwealth of Virginia* report is to provide a statewide perspective of information security program compliance across 114 agencies and institutions. This is the first report since our 2006 report, "*A Review of Information Security in the Commonwealth of Virginia*" that includes all 114 agencies in one report.

Overall, the Commonwealth's agencies and institutions of higher education continue their efforts to strengthen their information security programs while coping with the challenges of budget and staff reductions, and IT Infrastructure transformation activities.

Six (5 percent) of 114 agencies and institutions do not have an adequate information security program. Their weaknesses range from not having complete policies and procedures that employees can follow to safeguard mission critical and confidential data, to not providing adequate security awareness training. In general, small agencies with 100 or less employees have more compliance weaknesses to address than medium to large agencies or institutions of higher education.

The most predominant information security issue in the Commonwealth is employee computer access controls, followed closely by risk management and contingency plans. Twenty-eight (25 percent) out of 114 agencies and institutions do not have employee computer access controls that are compliant with the Commonwealth's standards or industry best practice. Twenty-seven (24 percent) do not have compliant risk management and contingency plans.

Findings

It is critical that agencies and insitutions put forth the necessary effort and resources to build a risk management approach to identify the fundamental safeguards that are right for their business environment. Without using a risk management approach, agencies and institutions will risk having too little (or too much) security controls. The result is a program that either does not sufficiently protect data or costs too much.

Lastly, during our information security reviews this past year, we continue to see that some agencies elect to maintain, at their own expense, local server rooms for the IT Partnership's servers. Without an adequate analysis of the costs involved to maintain physical and environmental security standards, room access administration, electricity, etc., agencies are not able to evaluate the true cost of keeping the IT Partnership's servers locally in the agency's building. The Virginia Information Technologies Agency is developing a process and template to assist in determining this cost and the template will be available in February 2011.

–TABLE OF CONTENTS–

INTRODUCTION

This report will show how well the Commonwealth's agencies and institutions of higher education build, maintain, and follow their information security programs, and how well these programs adhere to the Commonwealth's Information Security Standard (SEC501) and industry best practices. In other words, this report provides a Commonwealth-wide picture of Information Security Program compliance across agencies and institutions, and identifies common weaknesses in those security programs.

This is the fourth *Information Security in the Commonwealth* report issued by this Office since 2006[1]. The first report resulted in new legislation, issuance of an Executive Order, and new policies, procedures, and guidance issued by the Chief Information Officer (CIO) of the Commonwealth. Part of the new legislation changed the Commonwealth's focus on security, from executive branch agencies only to the entire Commonwealth, giving the CIO the authority to work with both the Legislative and Judicial Branches to ensure adequate Information Security. Subsequent reports have concluded that Information Security Programs within state agencies and institutions have shown overall improvement.

The Auditor of Public Accounts conducts security reviews throughout the year during regularly scheduled financial and performance audits of agencies and institutions of higher education. This report consolidates the most recent information security findings and issues our audits have found in 114 agencies and institutions of higher education. By consolidating this information, we can identify and analyze information security issues facing the Commonwealth across several agencies.

The IT Infrastructure Partnership (Partnership) operates and manages a significant portion of the IT infrastructure used by Commonwealth agencies. The Virginia Information Technologies Agency (VITA) oversees the contract between the Commonwealth and the Partnership service provider, Northrop Grumman (NG). Information security audits of the Partnership's IT Infrastructure hardware components, including firewalls, routers, switches, desktops, laptops, and servers, are outside the scope of this report. As part of the Partnership agreement, NG employs a public accounting firm to review and report on its information security over the infrastructure. VITA sets the scope of this review. For agencies participating in the Partnership, our reviews include application and database security, physical and environmental security, and agency security programs.

Additionally, we reviewed the agency server room transformation and migration process to determine what information is available to agencies as they make decisions whether to keep the Partnership's servers locally at the agency, or to move the servers to the Chester data center. For example, do agencies have sufficient information to consider the cost of maintaining a local server

[1] Previous reports are available on the APA website, www.apa.virginia.gov. In chronological order: *A Review of Information Security in the Commonwealth of Virginia*, December 1, 2006. *2008 Statewide Review of Information Security in the Commonwealth of Virginia*, December 12, 2008. *Commonwealth Information Security Implementation*, November, 2009.

room, including the physical and environmental controls, versus moving the servers to the Partnership's data center in Chester where these controls are included in the monthly server cost?

When reviewing individual agency information security programs, we make sure that the programs address any concerns and issues found by the public accounting firm conducting the review of the Partnership's operation and security. If we find a gap between the services provided by the Partnership and individual agency, our audit reports will address those issues.

Objectives

We had three objectives for this report.

1) Provide a statewide summary of information security program compliance across agencies and institutions of higher education.

2) Provide a statewide analysis of common security program compliance issues.

3) Review agency server room transformation and migration process for those agencies that participate in the Partnership.

Scope

The Office conducted field work for this report as part of our regularly scheduled audits of agencies and institutions of higher education. We reviewed the most recent audit reports for 114 agencies and institutions of higher education (see Appendix A).

Methodology

We reviewed agencies' information security programs to determine if they met two basic criteria for compliance. The first was to determine that the agency had essential security program components documented and that they meet the requirements of the Commonwealth's standards and industry best practices. The second was to determine whether the agency is following their security program.

The foundation of an information security program begins with an agency's risk management and contingency plans. Normally, these plans include the following documents.

1. Business Impact Analysis (BIA)
2. Risk Assessment (RA)
3. Continuity of Operations Plan (COOP)
4. Disaster Recovery Plan (DRP)

If properly developed, these documents provide the information an agency needs to write adequate policies and procedures for its information security program. However, if one of these documents is missing or poorly written, then the agency cannot develop the proper policies and procedures that guide the agency's employees in identifying and protecting sensitive data. In addition, agencies normally develop these documents in the order stated above. For example, agencies cannot develop a DRP that states the order in which an entity should restore information systems without first identifying and prioritizing their most critical business functions.

Once an agency has developed adequate risk management and contingency plans, the next step is to develop policies and procedures that the agency's staff can use to provide consistent protection of agency data. These policies and procedures have to meet the requirements of the Commonwealth's Information Security Standard (SEC 501), or for independent agencies and some institutions of higher education, an industry best practice, such as ISO 27002.

Our reviews compared the components of the agencies' information security program, including the four risk management and contingency plans, against the Commonwealth's Standards and industry best practices. Based on this comparison, we drew conclusions on the completeness and adequacy of the documented program. We then reviewed processes, configurations, and documentation to determine whether the agency follows its security program. This review resulted in conclusions on the effectiveness of the established security program.

We established the following rating criteria for this report.

Does the Agency have an adequate Information Security Program that effectively mitigates risks to mission-critical and confidential data?

Yes: The agency's program:

- Includes all risk management and contingency plans and essential components.
- Adequately addresses the requirements of the standards or best practices the agency follows.
- Includes communication to staff, and management has implemented and regularly monitors the plan for effectiveness.

No: The agency's program:

- Is missing one or more of the risk management and contingency plans or any of the other essential components.
- Does not adequately address the requirements of the standards or best practices the agency follows.
- Has not communicated the program to staff, and management has failed to either implement or regularly monitor the program for effectiveness.

Appendix A includes a detailed listing that summarizes each agency and institutions' security program weaknesses found during our reviews. We have determined whether each agency or institution has an adequate information security program, which we indicate with a "Yes" or "No" response. Having an adequate information security program does not mean that we have not made recommendations to improve or enhance the program. We discuss our findings below.

Our review of the agency server room transformation and migration process for Partnership agencies consisted of interviews with VITA staff, examination of the Comprehensive Infrastructure Agreement, and examination of monthly agency Partnership bills.

IMPORTANCE OF AN INFORMATION SECURITY PROGRAM

The goal of an information security program is to preserve the confidentiality, integrity, and availability of data through the implementation of rules and procedures. Protection of confidential information such as social security numbers, health records, and other personal information is important to citizens and the reputation of the Commonwealth. Sensitive data in the Commonwealth is not limited to the personal information of citizens; but it also includes financial information of agencies. In an era of strained budgets and increased government transparency, it is more important than ever to ensure that agency financial data is accurate and reliable.

The weakest link in securing data is the need for employees to access, store, change, and sometimes delete data. A strong security program works to strengthen that link by defining controls over who has access, how they get access, and what data a person can access. To obtain total data security, an entity would require that no one have access to data. Clearly, this scenario is impractical because agencies require employees to perform jobs that rely on access to data. Through the development and implementation of a security program, an agency can better control internal and external access to data and communicate their expectations of staff. An information technology security program does not guarantee total prevention of the compromising of systems and data; but it does make such compromise more difficult.

Security is not just keeping sensitive data out of the wrong hands. An information security program also provides assurance that staff and the public can access accurate data when they need it. Citizens count on government agencies to provide essential services at all times. In order to provide reliable services, agencies need to have the ability to quickly restore operations that depend on information systems in the event of a system outage. This is especially important during emergency situations such as natural disasters. The demand for information and government services increases dramatically during emergencies and agencies must have the ability to respond promptly.

MAINTAINING AN INFORMATION SECURITY PROGRAM

Strong information security programs do not stop upon completion of the documentation of risk management plans, contingency and recovery plans, or security policies and procedures. It is equally important to ensure constant updates and tests of plans, communication of security expectations to employees, and accountability for those expectations.

As agency technology environments change, so do the security risks. New technologies, new methods of communication, and the increased use of online services by citizens create new challenges for agencies in securing data. Because of this, security programs require regular reviews and updates to ensure they address the latest vulnerabilities.

While automated security controls are generally reliable and prevent users from circumventing certain security requirements, agencies must continuously inform system users of their responsibility for the security of the data they use. Users must have an awareness of their role in protecting critical data, the importance of complying with agency security policies and procedures, and how to respond if they suspect someone has compromised data. Once system users have an awareness of their need to maintain security of information, agencies can better enforce the requirements of their security programs and hold users accountable for compliance.

Agencies and institutions use their security programs to guide not only the use of automated security controls, but also manual controls that depend on employees to follow certain rules or procedures. The documentation, implementation, enforcement, and evaluation of these rules are key to maintaining strong security over critical data.

The figure below depicts the typical lifecycle of an information security program.

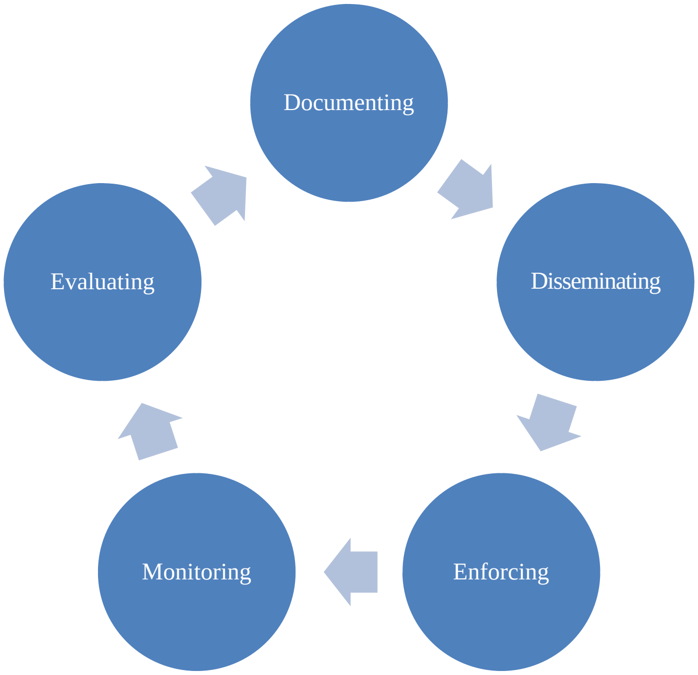


Figure 1. Information Systems Security Program Life Cycle

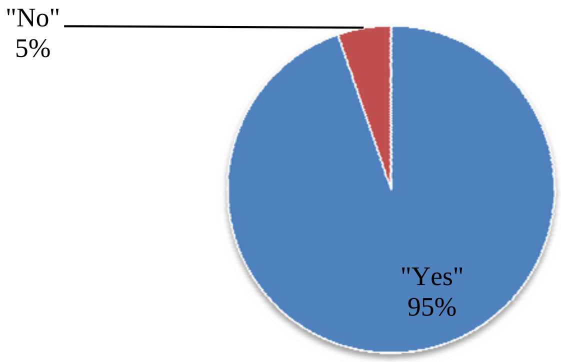
INFORMATION SECURITY SUMMARY REPORT

The Commonwealth's agencies and institutions continue their efforts to strengthen their individual information security programs while coping with the challenges of budget and staff reductions. These challenges hinder an agency's ability to update security programs to address changing risks, implement new technologies to mitigate risks, and provide the resources necessary to ensure information security remains a high priority. As a result, progress toward mature security programs has slowed. Overall, agencies view information security as a priority and understand the value information security programs.

We audited the information security programs of 114 agencies and higher education institutions. Our analysis shows that six of the 114 entities reviewed, or five percent, do not have adequate information security programs.

While there has been significant improvement in the number of agencies and institutions with adequate information security programs, we continue to find areas and issues that these entities need to improve.

Adequate Agency
Information Security Programs



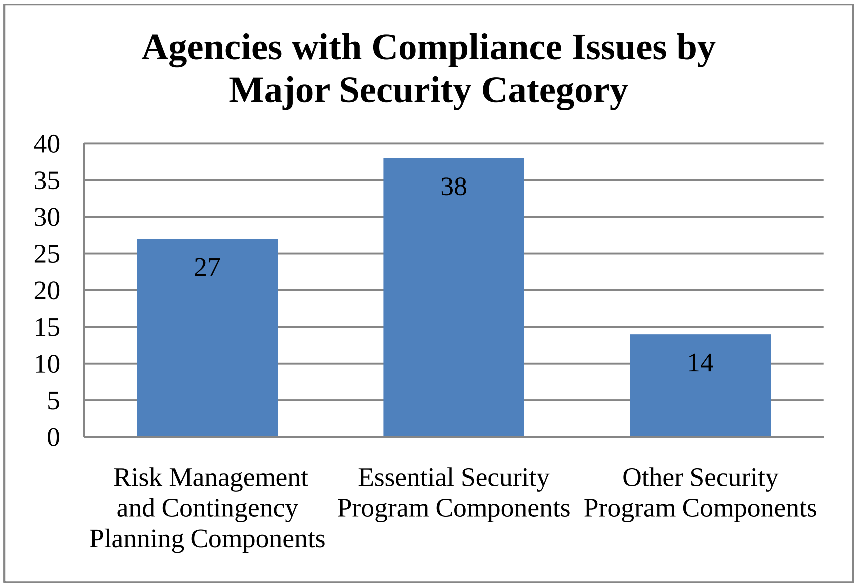
In order to identify trends and commonalities among these compliance issues, we have separated the security program components into the following major categories.

1. *Risk Management and Contingency Planning Components* comprised of the information technology risk assessment, business impact analysis, continuity of operations plan, and disaster recovery plan.

2. *Essential Security Program Components* comprised of seven critical elements of information security that guide or require certain practices designed to mitigate risks and protect mission-critical and confidential data.

3. *Other Security Progam Requirements* includes other areas required by best practices or the Commonwealth Standard important to a comprehensive security program.

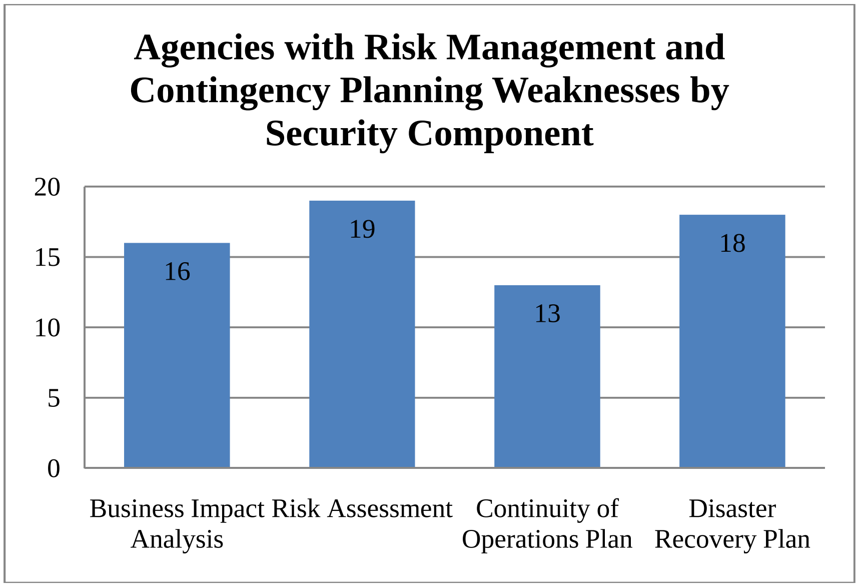
In our analysis, 27 agencies and institutions have weaknesses in the area of risk management and contingency planning, 38 have weaknesses in essential security program components, and 14 have weaknesses in other areas of their security program.



Next, we will analyze each of these major security categories, starting with Risk Management and Contingency Planning.

Risk Management and Contingency Planning

The following table illustrates the distribution of weaknesses in the area of risk management and contingency planning.

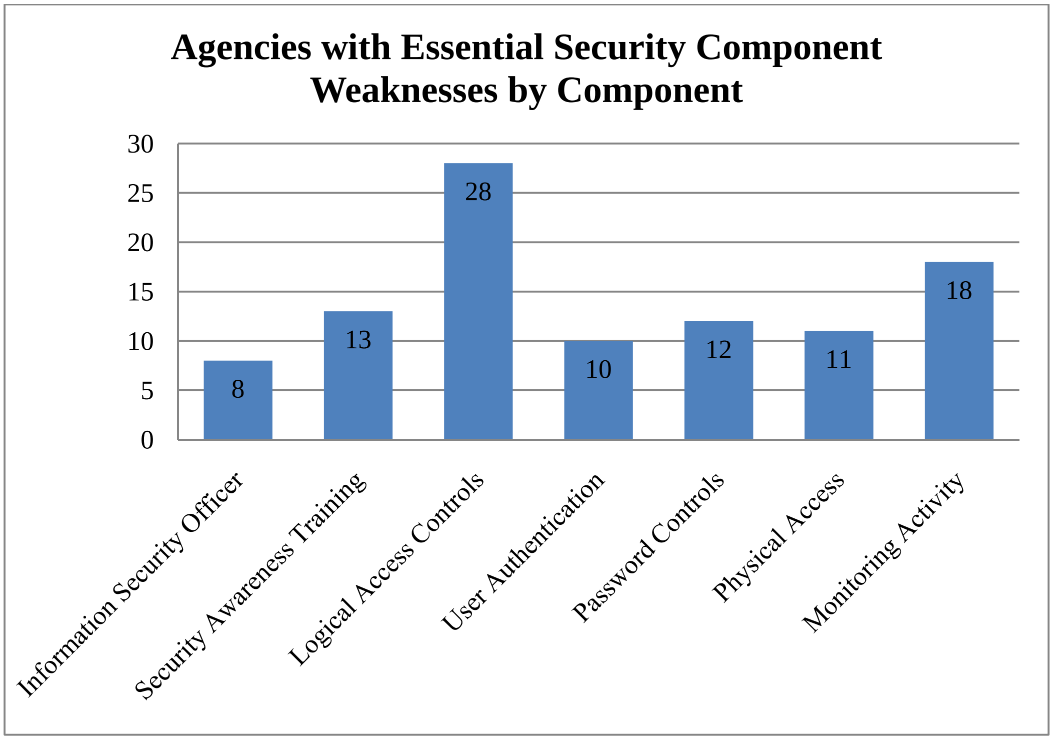


While most agencies and institutions reviewed during this period have adequate risk management and contingency plans, 27, or 24 percent, have failed to complete, update, or test these documents. Because agencies and institutions use these plans to determine where to focus systems security efforts, it is imperative that these documents contain accurate, specific, and thorough information to provide adequate support to the overall security program.

After identifying risks to systems and the impact of systems on business functions, an agency or institution can develop policies and procedures to address the areas of risk and other issues surrounding the most critical systems. These policies and procedures define management's expectations on how to protect confidential and critical data. Unfortunately, we found that the weakest component in agencies' and intitutions' risk management and contingency plans is the risk assessment. Twenty out of 114 agencies and institutions (18 percent) have incomplete or incorrect risk assessments. When developing these documents, agencies and institutions must ensure that they address all requirements in the standards or best practices they use.

Essential Security Program Components

The following table shows the distribution of weaknesses in essential security program components.



The majority of agencies and institutions reviewed have sufficiently documented and implemented these seven essential security program components. However, there is clearly one outlier in the group: logical access controls.

Logical access controls help prevent unauthorized use of sensitive data. With 28 out of 114 agencies and institutions (25 percent) not providing or exercising adequate logical access controls, this is the most problematic component in agencies' and institutions' security programs. These controls include the processes for requesting, approving, configuring, reviewing, and removing a user's ability to view, alter, or remove sensitive or critical data. When used in conjunction with strong authentication and password controls, good logical access management practices mitigate many of the risks associated with the types of data that agencies and institutions in the Commonwealth store in their systems.

The second of the top three essential security component weaknesses is monitoring activity. Monitoring system activity aids in determining if someone is accessing or attempting to access data inappropriately. In order to review the activity in systems or across networks, agencies and institutions must have the ability to maintain logs of events. We found that 18 out of 114 agencies and institutions (16 percent) do not comply with the Commonwealth's standards or best practices in monitoring system activity. Logs can track things such as access attempts, alterations to critical data, and suspected malicious activity. Not only should agencies and institutions log system activity, but more importantly, they should routinely review logs and respond appropriately to suspicious entries.

Lastly, agencies and institutions use security awareness training to inform and train employees of the security policies and procedures, new risks, and responsibilities for sensitive data they interact with daily. Fourteen out of 114 agencies and institutions (12 percent) do not perform adequate security awareness training. An effective security awareness training program provides employees with continuous communication of security issues, regular in-person or online classes, e-mail notices, and more technical, job-specific training, among other services.

Other Security Program Requirements

In addition to the elements discussed earlier, agency and institution security programs must address several other requirements of standards and best practices. In all, 14 agencies and institutions (12 percent) had weaknesses in these areas. The following is a list of the most common weaknesses in this category.

Component
Baseline Security Configurations
Data Sharing Security
Encryption
Incident Response Plan
Change Management
Vulnerability Scanning
Sanitation of Surplus Hardware
Security Reviews

FINDING #1:

The most predominant information security issue in the Commonwealth is logical access controls, followed by risk management and contingency plans. Twenty-eight (25 percent) out of 114 agencies and institutions do not have logical access controls that are compliant with the Commonwealth's security standards or industry best practices. Twenty-seven (24 percent) do not have compliant risk management and contingency plans.

Agency Server Room Transformation and Migration Process Review

During our information security audits this past year, we found that several agencies still operate local server rooms in order to accommodate the Partnership's servers. Maintaining decentralized server rooms incurs more than just costs to the Commonwealth for the space they take up and the electricity they use. It also incurs an additional expense to build and maintain the physical and environmental controls needed to protect the equipment and the mission-critical and confidential data they contain. These controls include, but are not limited to, key access systems, server-room monitoring, fire suppression, flood detection, and back-up electricity.

Agencies that use the Partnership for server, laptop, desktop, network, e-mail, disaster recovery, and technical support services have during the past several years undergone a transformation and migration process. The distinction between transformation and migration is the following.

> Transformation is when all of the Partnership's servers, laptops, desktops, network, e-mail, and disaster recovery services that the agency use transfer from the agency's old network to the Partnership's new network. The Partnership's network protects and remotely maintains the infrastructure at the agency location through its central network operations center located at the Partnership's data center in Chester.
>
> Migration is the physical relocation of an agency's server room to the Partnership's data center in Chester.

While the transformation process is mandatory for agencies participating in the Partnership, it is not mandatory for agencies to migrate servers to the Partnership's data center in Chester. Agencies should evaluate the costs of maintaining a local server room as part of their decision process to migrate.

FINDING #2:

Agencies should evaluate the total cost of maintaining the administrative, physical, and environmental controls for a local server room for the Partnership's servers and use this cost when evaluating the cost effectiveness of whether to maintain the Partnership's servers locally or to move the servers to the Chester data center.

The VITA is developing a process and template that will provide agencies with the ability to do a cost analysis of maintaining their server rooms. Using this cost analysis in conjunction with other network performance analyses, VITA can provide agencies with recommendations that consider the true costs associated with not migrating servers to the data center. VITA estimates these cost analyses to be available after the IT Infrastructure transformation is complete in February 2011.

CONCLUSION

Information security in the Commonwealth continues to face challenges as a result of difficult economic times and cuts in resources. While many agencies and institutions need to make improvements to their security programs, we did not find any agencies or institutions that had not made some effort to address information security. Better yet, a majority of agencies and institutions reviewed in this reporting period have compliant information security programs.

As identified in our last report, we continue to observe that agencies and institutions do not fully employ the *risk management* component of their information security programs. The risk management structure and process allows agencies and institutions to prioritize security needs and focus limited resources in areas of highest risk.

Over the past few years, agencies and institutions have improved their information security programs to meet the requirements of Commonwealth Standards and industry best practices. However as the programs mature, we begin to see that agencies and institutions do not regularly evaluate and revise their security programs. Because risks to electronic information constantly evolve, agencies and institutions must maintain security programs to mitigate the impact of those risks.

Lastly, for those agencies that participate in the IT Infrastructure Partnership, agency management should consider the true cost of maintaining a local server room when determining whether or not to move servers to the Partnership's data center in Chester. The Virginia Information Technologies Agency is developing a process and template to determine these costs.

Commonwealth of Virginia

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

Walter J. Kucharski, Auditor

November 15, 2010

The Honorable Robert F. McDonnell
Governor of Virginia

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

We are currently conducting audits of the information security programs for several agencies and submit our report entitled "**2010 State of Information Security in the Commonwealth of Virginia**" for your review.

We found that overall the Commonwealth's agencies and institutions of higher education are moving toward more stable and mature information security programs that comply with the Commonwealth's standards and industry best practices. In Appendix A, we have provided the status for 114 agency information security programs.

This progress report does not include new audit recommendations, but instead summarizes agencies' information security program progress, which was verified during normally scheduled audits.

Exit Conference and Report Distribution

We discussed this report with the Commonwealth's Chief Information Officer (CIO) on November 15, 2010. In addition, certain agencies elected to submit current status updates of their Information Security Program implementation progress. The Commonwealth's Chief Information Officer and agency 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:alh

Timothy M. Kaine
Governor

Viola O. Baskerville
Secretary of Administration

COMMONWEALTH of VIRGINIA

Department of Minority Business Enterprise
1111 East Main Street, Suite 300
Richmond, Virginia 23219

Samuel Hayes, III, PE
Director

November 5, 2009

The Honorable Walter J Kucharski
Auditor of Public Accounts
101 North 14th Street, 8th Floor
Richmond, VA 23219

RE: Semi-annual Commonwealth Information Security Implementation update

Dear Mr. Kucharski:

Thank you for the opportunity to provide you with an update regarding the improvement of information security program of the Department of Minority Business Enterprise.

In April 2009 review, the Auditor of Public Accounts findings cited that the Department of Minority Business Enterprise had no information security program. Since then, the DOA information Security Assistance Team has been providing us assistance in developing our information security program. Please find attached file for the report provided by the DOA information Security Assistance Team. According to this report, we have reached the point where we are in substantial compliance with the Commonwealth of Virginia Information Technology Resource Management Information Technology Security Standards (SEC 500-02 and SEC 501-01)

Again, thank you for the opportunity to provide an update for your information security report. Please don't' hesitate to contact me if you need any more information.

Sincerely,

Samuel Hayes III

Samuel Hayes III

COMMONWEALTH *of* VIRGINIA

DAVID A. VON MOLL, CPA
COMPTROLLER

Office of the Comptroller

P. O. BOX 1971
RICHMOND, VIRGINIA 23218-1971

October 21, 2009

MEMORANDUM

TO: Angela Chiang, Information Security Officer (ISO)
Department of Minority Business Enterprise (DMBE)

FROM: Joseph Kapelewski, Assistant Director
General Accounting, Information Security Assistance Team

SUBJECT: Information Technology (IT) Security Assistance Report

DOA's assistance to the DMBE has reached the point where you are in substantial compliance with the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Technology (IT) Security Standards (SEC 500-02 and SEC 501-01). Although not all elements of these standards are implemented, this is an opportunity to assess your progress with achieving that goal.

The attached report summarizes the key components of the IT Security evaluation and implementation as of August 17, 2009. Additionally, the appendices identify the compliance requirements of the Commonwealth's IT Security Standards and document the steps taken to meet those compliance standards.

The DOA Information Security Assistance Team will continue to support your Agency's information security efforts to achieve compliance with the "Standards". Therefore, this report is a progress update and not an end of service announcement.

Let me know if you have any questions as we continue to provide information security assistance to the VRC.

Attachments: Report and Appendices

cc: Lewis R. McCabe, Assistant State Comptroller
Department of Accounts
Matthew B. Teasdale, Information Security Specialist
General Accounting, Information Security Assistance Team

COMMONWEALTH *of* VIRGINIA

Andrew B. Fogarty
Interim Director

STATE COUNCIL OF HIGHER EDUCATION FOR VIRGINIA
James Monroe Building, 101 North Fourteenth Street, Richmond, VA 23219

(804) 225-2600
FAX (804) 225-2604
www.schev.edu

MEMORANDUM

TO: Walter J. Kucharski, Auditor of Public Accounts

FROM: Andrew Fogarty, Interim Director

DATE: November 9, 2010

SUBJECT: Response to Draft Copy of the *2010 State of Information Security in the Commonwealth of Virginia*

Thank you for the opportunity review the exposure draft of the report "*2010 State of Information Security in the Commonwealth of Virginia*" provided on November 3, 2010. In review of the report, we note that SCHEV is listed as not having an adequate information security program. We recognize that this finding is based on the audit that took place in March, 2009, approximately 18 months ago. In our response to that audit, SCHEV committed to working with "the Accounting and Internal Control Compliance Oversight unit at the Department of Accounts to develop an Information Systems Security Program." We did this and by January of 2010 we had completed this task.

In fact, on April 16, 2010, we received the attached memorandum from Joseph Kapelewski, Assistant Director, General Accounting, Information Security Assistance Team. It states, **"Based on our assessment, SCHEV is in substantial compliance with the Commonwealth of Virginia (COV) Information Technology Research Management (ITRM) Information Technology (IT) Standards (SEC 500-02 and SEC 501-01)."** Based on our understanding of the standards applied in your recent review, it seems that it would be appropriate to categorize SCHEV as something other than a "No", perhaps a "Yes*" given that its definition is: *An asterisk beside "Yes" means that while the agency's overall information security program adequately addresses and mitigates risk to mission critical and confidential data. However, the agency received one or more findings in their last audit report relating to information security.* We would appreciate your consideration of this proposed change.

SCHEV takes Information Security seriously and staff spent many hours working with Mr. Edward Miller from the Department of Accounts to put together an IT Security Program. We are in the process of revising it further to reflect the Agency's status "post-transformation."

Thank you for the opportunity to review and respond to this draft report.

Attachment

c: Ellie Boyd, Budget and Finance Director
Thomas Daley, Deputy Director
Tod Massa, Director of Policy Research and Data Warehousing

COMMONWEALTH *of* VIRGINIA

DAVID A. VON MOLL, CPA
COMPTROLLER

Office of the Comptroller

P. O. BOX 1971
RICHMOND, VIRGINIA 23218-1971

April 16, 2010

MEMORANDUM

TO: Tod Massa, Director, Policy Research and Data Warehousing
State Council of Higher Education for Virginia (SCHEV)

FROM: Joseph Kapelewski, Assistant Director
General Accounting, Information Security Assistance Team

SUBJECT: Information Technology (IT) Security Assistance Report

Based on our assessment, SCHEV is in substantial compliance with the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Technology (IT) Security Standards (SEC 500-02 and SEC 501-01). Although not all elements of these standards are implemented, this is an opportunity to assess your progress with achieving that goal.

The attached report summarizes the key components of the IT Security evaluation and implementation as of February 22, 2010. Additionally, the appendices identify the compliance requirements of the Commonwealth's IT Security Standards and document the steps taken to meet those compliance standards.

The DOA Information Security Assistance Team will continue to support your Agency's information security efforts to achieve compliance with the "Standards". Therefore, this report is a progress update and not an end of service announcement.

Electronic copies of all deliverables with hyperlinked attachments to detailed documents can be provided.

Attachment: Report and Appendices

cc: Lewis R. McCabe, Assistant State Comptroller
Department of Accounts
Goran G. Gustavsson, Audit Director, Information Systems Security
Auditor of Public Accounts
Edward Miller, Information Security Specialist
General Accounting, Information Security Assistance Team

ROBERT E. GLENN, President
ROANOKE
STEPHEN M. QUILLEN
LEBANON
ANITA O. POSTON
NORFOLK
GRADY K. CARLSON
MCLEAN
BRIAN K. JACKSON
RICHMOND

COMMONWEALTH of VIRGINIA
Virginia Board of Bar Examiners

W. SCOTT STREET, III
SECRETARY AND TREASURER
2201 W. BROAD STREET
SUITE 101
RICHMOND, VIRGINIA 23220

TELEPHONE (804) 367-0412
FAX (804) 367-0416

TEXT TELEPHONE CALLERS
USE VRC 1-800-828-1120

November 9, 2010

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

Re: Virginia Board of Bar Examiners
Information Security Program Update

Dear. Mr. Kucharski:

Thank you for the opportunity to provide an update on the development of the Information Security Program for the Virginia Board of Bar Examiners (the "Board").

The Board's staff members are currently working with the Department of Accounts' Security Specialist on a risk assessment that identifies controls for reducing risk to sensitive data. Once the risk assessment is finalized, the Board will create continuity plans to ensure that essential operations will be able to continue during and after potential disruption.

The Board's staff have also drafted IT security policies that address the requirements of the Commonwealth's security standards. Upon final approval by the Board, the policies will be implemented and all staff will undergo security awareness training.

With continued assistance from the Department of Accounts, the expected completion date for implementation of the Virginia Board of Bar Examiners' Information Security Plan is January 31, 2011.

Sincerely,

W. Scott Street, III
Secretary-Treasurer

WSS/mrw

Virginia's
Community Colleges

November 3, 2010

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

Dear Mr. Kucharski:

We are providing this letter in response to your advance draft copy of the *2010 State of Information Security in the Commonwealth of Virginia* report on the status of Information Security of the Virginia Community College System for the fiscal year ended June 30, 2009.

We confirmed receipt of the initial findings and recommendations on July 6, 2010 and attached our response and corrective action plan at that time.

We have remediated all findings for Dabney S. Lancaster Community College and Rappahannock Community College as indicated on the attached remediation report.

Please change the two (2) community colleges listed as YES* to YES, as VCCS is in full compliance.

If you have any questions, please contact Dave Mair, VCCS Controller, at (804) 819-4929.

Sincerely,

Glenn DuBois
Chancellor

cc: Dave Mair, Controller
James Davis, Information Technology Services

Donna VanCleave, Vice Chancellor for Administrative Services
Joy Hatch, Vice Chancellor for Information Technology

Dabney S. Lancaster Community College:

The security access has been changed so that employees that post accounts payable and revenue transactions in AIS will not have the capability to approve their own batches.

Implementation Date: July 1, 2010

Position Responsible: Business Manager and AIS Security Officer

Rappahannock Community College:

Currently all business office staff have the AIS roles to create and post batches for cross-training to ensure office coverage with a small staff and continuity of operations during disasters or pandemics. To enhance the segregation of duties as defined by the APA audit, roles were modified in AIS so that individuals who post accounts payable and revenue transactions do not have the capability to approve their own batches.

Implementation Date: July 15, 2010

Position Responsible: VP Finance & Administration and Business Manager

COMMONWEALTH of VIRGINIA

Samuel A. Nixon, Jr.
CIO of the Commonwealth
E-mail: cio@vita.virginia.gov

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

TDD VOICE -TEL. NO.
711

November 17, 2010

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' *2010 State of Information Security in the Commonwealth of Virginia* report. The report accurately reflects the significant progress made by agencies of the Commonwealth in creating and operating compliant information security programs, as well as highlighting key areas where more work is needed.

The pursuit of information security is a never-ending task driven by advances in technology and the evolution of threats. We agree with the first finding of the report that risk management should be a core component of the strategy that the Commonwealth uses to prioritize and justify security expenditures. To this end, the Virginia Information Technologies Agency (VITA) has been working to create a risk management program and an associated set of requirements for promulgation to and adoption by Commonwealth agencies.

Furthermore, we strongly agree with the second finding of the report - that agencies can reduce their total cost of ownership by consolidating outlying data centers to the Commonwealth Enterprise Solutions Center. VITA remains committed to providing agencies with the tools necessary to make an informed financial decision. While recognizing that hardware consolidation and virtualization will provide economic advantages to the Commonwealth, these steps have also proven to reduce security exposure, improve compliance and provide a common set of controls to mitigate risks to consolidated resources.

We are pleased with the progress reflected in this report and remain dedicated to strengthening the information security posture of the Commonwealth. As always, we appreciate the professionalism of your staff.

Sincerely,

Sam Nixon

Samuel A. Nixon, Jr.

c: The Honorable James D. Duffey, Jr., Secretary of Technology
Aaron Mathes, Deputy Secretary of Technology

APPENDIX A: Agency Information Security Program Compliance

***** An asterisk beside "Yes" means that while the agency or institution's overall information security program adequately addresses and mitigates risk to mission critical and confidential data, the agency or institution received one or more findings in their last audit report relating to information security. Our audit reports are available on the APA website, http://www.apa.virginia.gov. Click on the "Reports" link.

	Audit Report Issue Date	**2010 Security Program Compliance**
Agencies		
Attorney General and Department of Law	10/08/2010	Yes
Board of Accountancy	01/29/2010	Yes
Board of Bar Examiners	12/10/2009	No
Center for Innovative Technology	10/16/2009	Yes
Commonwealth's Attorneys' Services Council	03/26/2009	Yes
Compensation Board	10/15/2009	Yes
Department for the Aging	12/10/2008	Yes*
Department of Accounts - Division of State Internal Auditor	01/12/2010	Yes*
Department of Agriculture and Consumer Services - Division of Charitable Gaming	04/28/2010	Yes
Department of Alcoholic Beverage Control	10/18/2010	Yes*
Department of Aviation	12/15/2009	Yes
Department of Behavioral Health and Developmental Services - Catawba Hospital - Central State Hospital - Central Virginia Training Center - Commonwealth Center for Children and Adolescents - Eastern State Hospital - Hiram W. Davis Medical Center - Northern Virginia Mental Health Institute - Northern Virginia Training Center - Piedmont Geriatic Hospital - Southeasters Virginia Training Center - Southern Virginia Mental Health Institute - Southside Virginia Training Center - Southwestern Virginia Mental Health Institute - Southwestern Virginia Training Center - Virginia Center for Behavioral Rehabilitation - Western State Hospital	12/09/2009	Yes*
Department of Business Assistance	10/27/2010	Yes*
Department of Conservation and Recreation	06/14/2010	Yes*

	Audit Report Issue Date	**2010 Security Program Compliance**
Department of Correctional Education	04/14/2009	Yes*
Department of Corrections - Virginia Parole Board	05/10/2010	Yes*
Department of Criminal Justice Services	03/26/2010	Yes
Department of Education	11/17/2009	Yes
Department of Emergency Management	01/26/2010	Yes
Derpartment of Employment Dispute Resolution	01/06/2009	Yes
Department of Environmental Quality	05/12/2010	Yes
Department of Fire Programs	01/29/2010	Yes*
Department of Forensic Science	06/21/2010	Yes*
Department of Forestry	04/07/2009	No
Department of Game and Inland Fisheries	09/17/2009	Yes*
Department of General Services	05/08/2009	Yes*
Department of Health	12/09/2009	Yes*
Department of Health Professions	12/09/2009	Yes
Department of Historic Resources	03/08/2010	Yes*
Department of Human Resource Management	02/20/2009	Yes*
Department of Housing and Community Development	10/21/2009	Yes
Department of Juvenile Justice	03/11/2009	Yes
Department of Labor and Industry	10/26/2009	Yes
Department of Medical Assistance Services	12/09/2009	Yes
Department of Military Affairs - Virginia Defence Force	06/12/2008	No
Department of Mines, Minerals, and Energy	03/19/2009	Yes*
Department of Minority Business Enterprises	03/10/2009	No
Department of Motor Vehicles	12/15/2009	Yes*
Department of Planning and Budget	11/20/2009	Yes
Department of Professional and Occupational Regulation	10/07/2009	Yes*
Department of Rail and Public Transportation	12/15/2009	Yes
Department of Rehabilitative Services - Department for the Deaf and Hard-of-Hearing - Departmnet of the Blind & Vision Impaired - Virginia Board for People with Disabilities - Virginia Industries for the Blind - Virginia Rehabilitation Center for the Blind - and Vision Impaired - Woodrow Wilson Rehabilitation Center	12/2010[a]	No
Department of Social Services - Virginia Council on Child Day Care - and Early Childhood Programs	12/09/2009	Yes*
Department of State Police	03/24/2010	Yes*
Department of Taxation	01/12/2010	Yes*

	Audit Report Issue Date	2010 Security Program Compliance
Department of the Trasury	01/12/2010	Yes
Department of Transportation	12/15/2009	Yes
Department of Veterans Services - Sitter and Barefoot Veterans Care Center - Virginia Veterans Care Center	04/08/2010	Yes*
Frontier Culture Museum of Virginia	03/23/2010	Yes
Gunston Hall	05/10/2010	Yes
Indigent Defense Commission	03/16/2009	Yes*
Jamestown-Yorktown Foundation / Jamestown 2007	05/19/2010	Yes*
Library of Virginia	02/02/2009	Yes
Marine Resources Commission	02/26/2009	Yes
Motor Vehicle Dealer Board	12/15/2009	Yes
Potomac River Fisheries Commission	04/12/2010	Yes
Science Museum of Virginia	04/23/2010	Yes
Southwest Virginia Higher Education Center	06/21/2010	Yes
State Board of Elections	04/10/2009	Yes*
State Corporation Commission	10/08/2009	Yes*
State Council for Higher Education for Virginia	03/18/2009	Yes*
State Lottery Department	09/08/2010	Yes
Supreme Court (Judicial Department) - Court of Appeals of Virginia - Judicial Inquiry and Review Commission - Virginia Criminal Sentencing Commission	06/10/2010	Yes*
Virginia College Savings Plan	12/14/2009	Yes
Virginia Commission for the Arts	08/11/2009	Yes
Virginia Economic Development Partnership - Virginia National Defece Industrial Authority - Virginia Tourism Authority	10/21/2009	Yes
Virginia Employment Commission	12/01/2009	Yes*
Virginia Information Technologies Agency	07/13/2009	Yes*
Virginia Museum of Fine Arts	08/01/2008	Yes
Virginia Museum of Natural History	08/01/2010	Yes*
Virginia Office for Protection and Advocacy	04/01/2009	No
Virginia Port Authority	12/15/2009	Yes
Virginia Retirement System	12/02/2009	Yes*
Virginia State Bar	12/10/2009	Yes
Virginia Workers' Compensation Commission	11/17/2009	Yes*
Colleges and Universities		
Christopher Newport University	06/01/2010	Yes*
College of William and Mary - Richard Bland College - Virginia Institute of Marine Science	04/12/2010	Yes

	Audit Report Issue Date	2010 Security Program Compliance
George Mason University	04/19/2010	Yes
James Madison University	03/26/2010	Yes
Longwood University	05/26/2010	Yes*
Norfolk State University	06/17/2010	Yes*
Old Dominion University	03/05/2010	Yes
Radford University	04/14/2010	Yes
University of Mary Washington	04/27/2010	Yes*
University of Virginia Academic Division - University of Virginia's College at Wise	11/20/2009	Yes
University of Virginia Medical Center	11/20/2009	Yes
Virginia Commonwealth University	12/04/2009	Yes
Virginia Community College System	06/25/2009	Yes
- Blue Ridge Community College		Yes
- Central Virginia Community College		Yes
- Dabney S. Lancaster Community College		Yes*
- Danville Community College		Yes
- Eastern Shore Community College		Yes
- Germanna Community College		Yes
- J. Sargeant Reynolds Community College		Yes
- John Tyler Community College		Yes*
- Lord Fairfax Community College		Yes
- Mountain Empire Community College		Yes
- New River Community College		Yes
- Northern Virginia Community College		Yes*
- Patric Henry Community College		Yes
- Paul D. Camp Community College		Yes
- Piedmont Virginia Community College		Yes
- Rappahannock Community College		Yes*
- Southside Virginia Community College		Yes
- Southwest Virginia Community College		Yes
- Thomas Nelson Community College		Yes
- Tidewater Community College		Yes
- Virginia Highlands Community College		Yes
- Virginia Western Community College		Yes
- Wytheville Community College		Yes
Virginia Military Institute	04/29/2010	Yes
Virginia Polytechnic Institute and State University	11/05/2009	Yes
Virginia State University	06/23/2010	Yes*

[a] Rating is based on a report that we expect to issue in December 2010.

Total "Yes" & "Yes*": 108 agencies
Total "No": 6 agencies