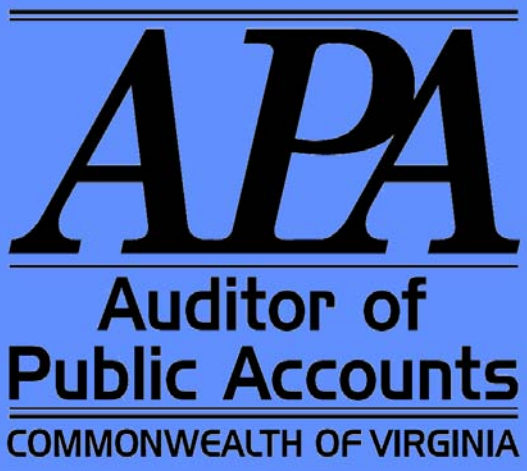
COMMONWEALTH INFORMATION SECURITY IMPLEMENTATION SEMI-ANNUAL UPDATE

NOVEMBER 2009



EXECUTIVE SUMMARY

The Commonwealth's agencies and institutions of higher education continue to strengthen their individual information security programs. Our office performed security audits at 54 agencies during the period December 1, 2008 through September 30, 2009.

While the overall assessment indicates that the Commonwealth is moving towards a more stable and mature information security program, small agencies (less than 100 positions) continue to receive poor marks. Out of 13 small agencies included in this report, eight (62 percent) do not have the essential information security program components that enables the agency to successfully follow a robust program that is built on standards and best practices.

In contrast, 39 (95 percent) of the 41 medium and large agencies and institutions included in this review have the essential components in their programs and comply with the standards and best practices.

Overall, 44 small, medium, and large agencies have either complete or partially complete programs. Thirty-six (82 percent) of the 44 agencies and institutions have complete programs and are successfully following their programs and training their employees. Ten agencies have basically no programs, since they are missing essential standards or best practice components and are not training employees or keep their programs updated.

A common weakness we have found during our audits is that agencies have not put forth the necessary effort and resources to build a security program that uses a risk management approach to identify the fundamental safeguards that is right for their business environment. Without using a risk management approach, agencies 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.

The Commonwealth has hired two Information Security Officers to establish a program and provide expertise and training for small agencies. Recently, they completed updating the security programs and provide training for several small agencies. We will start reviewing these programs during our upcoming audits.

Lastly, we expect to issue the next semi-annual report in April 2010; covering agencies audited during the six-month period October 1, 2009 through March 31, 2010 (see Appendix B).

– T A B L E O F C O N T E N T S –

INTRODUCTION

This is the first semi-annual report that this Office will issue on the Information Security Programs in the Commonwealth. In the past three years, we have issued two statewide reviews on the Status of Information Security in the Commonwealth. The first report resulted in legislation, issuance of an Executive Order, and new policies, procedures and guidance issued by the Chief Information Officer (CIO). The first review also changed the Commonwealth's focus on security from agency specific to the entire Commonwealth, giving the CIO the authority to work with both the Legislative and Judicial Branches of government to ensure adequate Information Security. The second review found an improvement in the overall Information Security Program within state agencies and institutions.

Since we conduct our Information Security Reviews during our annual audits of agencies and institutions, the Auditor of Public Accounts will issue a semi-annual report, which will provide information on the agencies and institutions reviewed during a six-month period. This first semi-annual report, however, will include agencies and institutions audited during the period December 1, 2008 through September 30, 2009. This 10-month period will provide coverage for agencies and institutions audited since we issued the "2008 Statewide Review of Information Security in the Commonwealth of Virginia" in December 2008. The next semi-annual review will cover audits completed during the six-month period October 1, 2009 through March 31, 2010.

A significant portion of the Commonwealth Security Program centers on the information technology infrastructure, including communication infrastructure provided to the Commonwealth agencies by Virginia Information Technologies Agency (VITA) and their partnership with Northup Grumman (Partnership). The Partnership employs a certified public accounting firm to conduct a review of its operation and security of the information technology infrastructure. The firm provides a copy of their assessment to VITA and this Office. The Auditor of Public Accounts works with VITA information security staff to help determine the scope of the work performed by the firm, and to ensure that there is appropriate consideration to protecting all of the Commonwealth agencies and institutions receiving services from the Partnership.

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 and we will include them in our semi-annual reports.

An information technology security program does not guarantee that someone will not be able to compromise an agency's systems. The security program is a combination of risk assessment, internal insurance, employee awareness and training, and emergency procedures to follow in a disaster. The information technology security program does not prevent, but slows down or makes it extremely difficult to compromise an entity's system and data. It provides a plan and backup when a disaster or breach occurs.

This semi-annual status report summarizes whether the Commonwealth's agencies and institutions of higher education have built information security programs that adhere to the Commonwealth's Information Security Standard (SEC 501) and industry best practices. We also

summarize whether agencies and institutions of higher education are following the requirements of their information security programs by providing training and communicating expectations to their employees.

When evaluating whether agencies have adequate information security programs, it is important to realize that just documenting risk management plans, continuity of operations plans, and security policies and procedures are only half the effort. It is equally as important to have a routine to constantly update the plan and communicate expectations employees.

Overall, the Commonwealth's agencies and institutions of higher education continue to improve their information security programs. Several factors contribute to the speed at which agencies' information security programs progress. For example, while larger agencies often have the expertise to maintain an information security program, the agency's complexity often makes fast progress difficult. On the other hand, smaller agencies may not be as complex; however, they often lack their own expertise to develop a security program and train its employees.

Maintaining an Information Security Program

Unfortunately, developing an information security program is a process without an end. An agency's information security program is a living document that needs to change at the same speed as the agency and its programs change. This is especially true during tough economic times. As agencies change their business processes to become more efficient, agencies simultaneously need to update their information security programs and train their employees. In this dynamic environment, we also need to add the fact that data can never become 100 percent secure.

Data that is 100 percent secure is an impossibility, no matter how many security controls are put in place to protect the data. It is true that data will be *more* secure if more controls are put in, but keep in mind that the *more* secure data is made, the more difficult and costly it will become to manage and use. This is a contradiction to the main purpose for using computers in the first place – to be more productive and cost efficient. This process begs the question: "How much security is enough?"

The answer is the same as is given many times when answering Information Technology related questions: "It depends." According to industry best practices, the security controls around your data should be determined by evaluating three factors – *confidentiality, integrity,* and *availability*.

Confidentiality, integrity, and availability are the main factors considered when defining the sensitivity of your data, and how many security controls you need to put in place to achieve reasonable protection. This determination is part of the risk management process, which is the foundation of an information security program that provides "enough" security. With a clear picture of which IT systems contain which types of data, and what the business expectations are for the integrity and availability of that data, agencies can make sure that investments in information security are done wisely and effectively.

Objectives

We had three objectives for this report.

1) Provide a statewide summary of whether agencies and institutions of higher education have developed a security program based on the Commonwealth's Information Security Standard or industry best practices.

2) Provide a statewide summary of whether agencies and institutions of higher education are following their information security programs.

3) Analyze the progress made by agencies and institutions of higher education.

Scope

The Office conducted field work for this report between December 1, 2008 and September 30, 2009 as part of our agencies' and institutions of higher education's regularly scheduled audits. During this period, we reviewed the information security programs and issued audit reports for 54 agencies and institutions of higher education (see Appendix A).

METHODOLOGY

We reviewed agencies' information security programs in two parts. The first part of the review determined whether agencies are developing their programs based on the Commonwealth's Information Security Standard or industry best practices, depending on applicability to the individual agency. The second part of the review determined whether the agencies' are following their programs.

Review: Part 1. Developing an Information Security Program

The foundation of an information security program begins with an agency's risk management and continuity of operations 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 in order 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, it is very difficult (and often confusing) to start developing a COOP that states the order in which an entity should restore business functions without first identifying an agency's risks in a risk assessment.

Once an agency has developed adequate risk management and continuity of operations 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. In our review, we looked at seven essential components.

1. An organizational structure that includes the assignment of an Information Security Officer (ISO)
2. A formal training program
3. Policies and procedures for approving logical access
4. A process requiring user authentication for access to all systems and management approval of any exceptions after having evaluated the risks of those exceptions
5. Policies and procedures regarding password controls
6. Appropriate physical safeguards in place to protect all the critical and sensitive assets against unauthorized access and documentation of who approves these controls
7. Active monitoring of their systems, applications, and databases

In our review, we compared the agencies' seven essential information security components and the four risk management and continuity of operation plans, against the Commonwealth's Standards and industry best practices. We established the following rating criteria.

Does the Agency have an Information Security Program that complies with Best Practices?

Yes: The agency has performed a security analysis and documented a program that includes all risk management and continuity of operations plans and all seven essential components.

No: The agency is missing one or more of the risk management plans, continuity of operations plan, or essential components.

Review: Part 2. Following an Information Security Program

Documenting information security policies and procedures is a great start in providing consistent and reasonable protection of confidential and mission critical data. However, the best policies and procedures are useless unless management keeps them updated to reflect the current business environments, and employees are aware and trained in their responsibilities.

The second part of our review address whether agencies and institutions of higher education have adequately implemented their security programs into their organizations. We established the following rating criteria.

Does the Agency follow its Information Security Program?

Yes: The agency is following and has established a process to update its information security program and provide adequate training to its employees.

No: The agency is not fully following the requirements of its information security program.

N/A: The agency does not have a security program that complies with best practices, and the agency has a "No" rating in part 1, "The Agency has a Security Program that complies with Best Practices."

Please refer to Appendix A for a detailed listing that outlines position level, last audit, security finding(s) flag, best practice compliance, and whether each agency follows its security program.

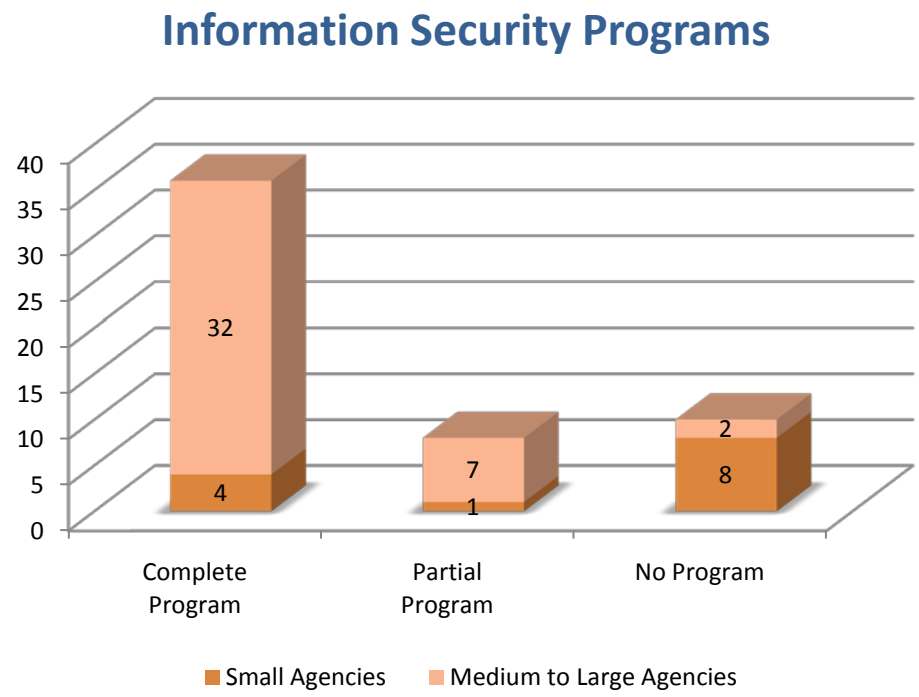
INFORMATION SECURITY PROGRESS REPORT

The Commonwealth's agencies continue to strengthen their individual information security programs. As a result, the agencies are better at safeguarding confidential and mission critical data, reducing the data's likelihood of being compromised, becoming inappropriately available, or being of poor quality. While agencies have had their budgets significantly reduced due to the current economy, we are encouraged to see that most agencies prioritize their information security programs, and see the value in managing risk and planning for continuing the agency's program(s) in case of a disaster or catastrophe.

During the 10-month period, December 1, 2008 through September 30, 2009, we audited the information security programs of 54 small, medium, and large agencies. For analysis purposes, we divide agencies' information security program progress into three categories.

Complete Program	The agency's information security program complies with best practices and the agency is following and has established a process to update its information security program and provide adequate training to its employees.
Partial Program	The agency's information security program complies with best practices, but the agency *does not* follow, update, or adequately train its employees.
No Program	The agency's information security program *does not* comply with best practices and, therefore, *does not* have adequate processes to follow, update, or adequately train its employees.

In our analysis, 36 agencies have complete programs, eight agencies have partial programs, and 10 agencies have no programs. The following graph illustrates the distribution and a distinction of small agencies versus medium and large agencies in each category.



Overall, for small, medium, and large agencies, 10 out of 54 agencies (19 percent) do not have information security programs that comply with the Commonwealth's standards or industry best practice. Without a compliant and complete information security program, it is almost impossible for these agencies to teach their employees to follow consistent policies and procedures designed to protect the Commonwealth's data.

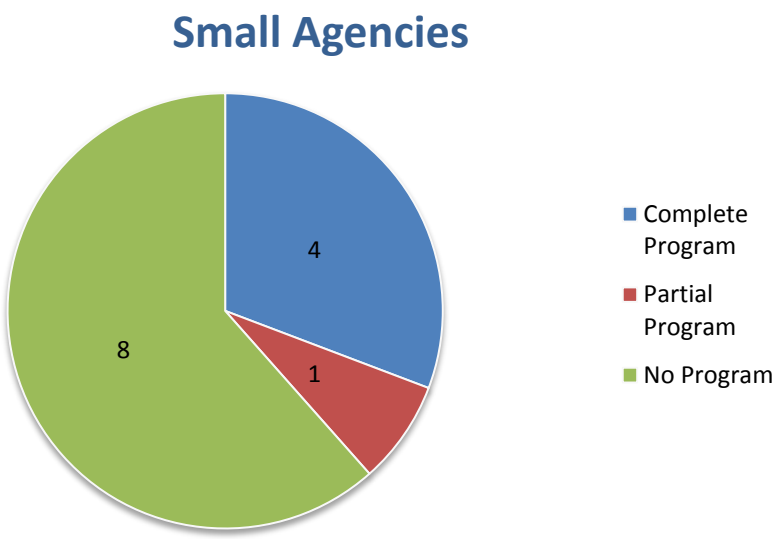
The remaining 44 agencies have developed compliant information security programs and 36 agencies (82 percent) have trained their employees and follow their respective information security programs. Eight agencies (18 percent) have an adequate security program, but have failed to successfully implement the program and train the employees.

While we have seen some improvements in small agencies' information security programs, our main concern is still that small agencies do not have the resources to establish and maintain their security programs.

Out of the 13 small agencies included in this report, only four (31 percent) have complete programs. Three of the four small agencies that now have and maintain information security programs that comply with the standards have significant non-general fund resources that allow them to employ consultants and other resources to develop and implement their programs. One of the 13 small agencies has a partial program where the agency has not fully implemented the program and trained its employees.

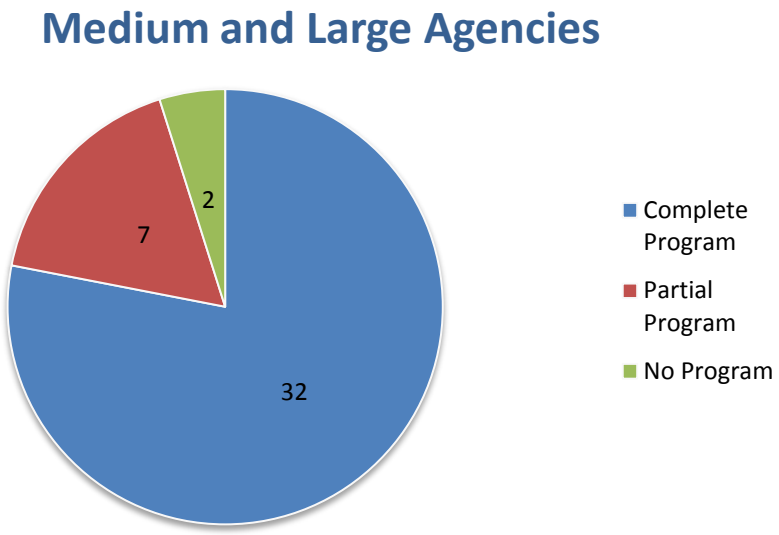
The reason the remaining eight (62 percent) agencies have not developed and implemented an information security program arises from their inability to employ consultants or maintain a staff

of information security professionals. The following graph illustrates small agencies' progress towards developing an information security program.



The Commonwealth hired two full-time Information Security Officers in July 2008 to assist small agencies in developing information security programs. As these Information Security Officers complete the information security programs for these agencies, and provide training to their staff, we expect a significant improvement in small agencies' information security programs.

In comparison to small agencies, out of 41 medium and large agencies included in this report, thirty-two (78 percent) have complete programs. Seven (17 percent) have partial programs where the agencies have not fully implemented the program and trained its employees. The following graph illustrates medium and large agencies' progress towards completing their security programs.



This result reflects emphasis that the Governor and Secretary of Technology have placed on information security programs, as well as some highly publicized information security breaches.

Currently, medium and large agencies appear to have continued to commit the financial resources to maintaining and updating their information security programs.

CONCLUSION

The Commonwealth's information security posture continues to improve despite difficult economic times and sparse resources. While small agencies are still behind in developing information security programs that follow the Commonwealth's security standards and industry best practices, several of these agencies are receiving assistance from the Information Security Officers assigned to small agencies. We anticipate reviewing these programs during our upcoming audits.

We have seen one common information security program component that many agencies and institutions underutilize – Risk Management. A solid risk management structure and process can save resources and spare embarrassment for an agency in the long run. Without evaluating the data and its risk, there is a very small chance that an agency will be able to adequately protect that data. The data will either have too much protection (too costly), or too little protection (embarrassing and costly if breached).

Commonwealth of Virginia

Walter J. Kucharski, Auditor

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

November 6, 2009

The Honorable Timothy M. Kaine
Governor of Virginia

The Honorable M. Kirkland Cox
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 "**Commonwealth Information Security Implementation – Semi-Annual Update**" for your review.

We found that overall the Commonwealth's agencies 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 54 agency information security programs. The next semi-annual update report is scheduled to be issued in April, 2010, and will include agencies audited during the period October 1, 2009 through March 31, 2010.

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 4, 2009. 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

WJK:alh

COMMONWEALTH of VIRGINIA

Department for the Aging

Linda L. Nablo, Commissioner

November 4, 2009

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

Dear Mr. Kucharski:

The Department for the Aging (VDA) appreciates the opportunity to provide an update on the Auditor of Public Accounts' (APA) finding that VDA needs to strengthen its information security program. Specifically, APA's measurement of a security program that complies with best practices found that VDA had not performed a Business Impact Analysis (BIA) and a Risk Assessment (RA).

VDA has acquired the services of the Department of Accounts (DOA) to help develop the needed documentation. The DOA staff that assists small agencies has been a valuable asset to help us move forward with these tasks and we are grateful for their assistance. I am pleased to be able to inform you that VDA now has a working BIA and has begun the tasks necessary to develop the RA, which should be finalized in January 2010.

As noted in the original finding, VDA is a small state agency. The agency acquires most of its IT resources through outside vendors. VDA continues to contract with these services in full compliance with VITA's standards and requires all of its contractors to adhere to the Commonwealth's Information Security Policy, Standards, and Guidelines.

1610 Forest Avenue, Suite 100, Richmond, Virginia 23229
Toll-Free: 1-800-552-3402 (Voice/TTY) · Phone: 804-662-9333 · Fax: 804-662-9354
E-mail: aging@vda.virginia.gov · Web Site: www.vda.virginia.gov

DIGNITY · INDEPENDENCE · SECURITY

Virginia department for the Aging

Again, thank you for the opportunity to provide an update on the status of this finding and please contact me if you require further information.

Very Truly Yours,

Linda Nablo

Linda Nablo
Commissioner

Cc: David A. Von Moll, Comptroller, Department of Accounts

COMMONWEALTH of VIRGINIA

Department of Criminal Justice Services

Leonard G. Cooke
Director

1100 Bank Street
Richmond, Virginia 23219
(804) 786-4000
TDD (804) 786-8732

November 4, 2009

Auditor of Public Accounts
Attn: Mr. Goran Gustavsson
Audit Director – Information Systems Security
101 North 14th Street
Richmond, VA 23219

Dear Mr. Gustavsson:

This is a follow-up to the March 10, 2009 corrective action for our 2008 audit finding. Over the last few months the Department of Criminal Justice Services has completed a review and revision of its Continuity of Operations Plan (COOP) and Business Impact Analysis (BIA).

The business functions of the Department were analyzed and documented in the BIA. Following this effort, the COOP was revised to insure that both documents accurately reflect the critical business functions of the Department.

Additionally, the Department has requested of the VITA/NG Partnership, both verbally and through the completion of a formal Request for Services (RFS), assistance in testing the Disaster Recovery provisions contained within the COOP.

The revised COOP, BIA and documentation for Disaster Recovery testing assistance were forwarded to Ms. Linda Wade, the APA's Audit Director for our Department, on October 16, 2009. Please include this response in your semi-annual report.

Sincerely,

Leonard G. Cooke
Director

COMMONWEALTH of VIRGINIA

Department of Emergency Management

MICHAEL M. CLINE
State Coordinator

JANET L. CLEMENTS
Chief Deputy Coordinator

BRETT A. BURDICK
Deputy Coordinator

10501 Trade Court
Richmond, Virginia 23236-3713
(804) 897-6500
(TDD) 674-2417
FAX (804) 897-6506
www.vaemergency.com

November 5, 2009

Goren Gustavsson
Audit Director - ISS
Commonwealth of Virginia
Auditor of Public Accounts
Monroe Building, 101 North 14th Street
Richmond, VA 23219

Subject: FY09 SSA Findings

Dear Mr. Gustavsson:

In 2008 the Auditor of Public Accounts (APA) findings found that Virginia Department of Emergency Management (VDEM) was not following our security protocol. However, we have made many changes within our agency to not only establishing information security policies but to also implement them throughout the past year. All employees are required to take an Information Technology security awareness quiz each year to make them aware of how to protect our network. We have also required employees to fill out access request forms for network access and network share access. For more complex systems such as our crisis management system we have a more intense vetting process.

We welcome the APA to visit our facility to see the changes we have implemented at VDEM throughout the past year.

Sincerely,

Michael M. Cline

MMC/BA/bcf

COMMONWEALTH of VIRGINIA

W.G. Shelton, Jr.
EXECUTIVE DIRECTOR

Virginia Department of Fire Programs

1005 Technology Park Drive
Glen Allen, VA 23059-4500
Phone: 804/ 371-0220
Fax: 804/ 371-3444

November 3, 2009

Auditor of Public Accounts
Post Office Box 1295
Richmond VA 23218

The Department of Fire Programs appreciates the opportunity to provide a progress update of the audit finding cited in the Auditor of Public Accounts' audit report for the two-year period ended June 30, 2008, and consideration of our management update to be included in the Commonwealth Information Security Semi-Annual Update 2009 Report.

BRIEF BACKGROUND:

APA Audit Finding (March 2009): Strengthen Information Systems Security Program
The Department of Fire Programs (Fire Programs) has improved its information security program since our last audit, but there are some key components that still require strengthening to be fully compliant with the Commonwealth's information security standards. Fire Programs has performed a business impact analysis and risk assessments of identified systems; however, they have not developed a continuity of operations plan or disaster recovery plan.

Fire Programs is working with the Accounting and Internal Control Compliance Oversight unit at the Department of Accounts (Accounts) in developing an information systems security program. They anticipate completing their program in May 2009 and should ensure they address the items noted above in their final plan.

Management Response (March 2009): Strengthen Information Systems Security Program
The agency is committed to complying with the SEC 501 Security Standard. The agency is dependent on the VITA/Northrup-Gruman partnership to provide services contained in the standards to which the agency is held accountable. Fire Programs continues to work collaboratively with the partnership to move forward on compliance concerns. The agency has realigned agency staff to partner with both the Department of Accounts and VITA/Northrup-Gruman staff to complete the comprehensive requirements contained in those documents.

As cited, the agency has already completed the business impact analysis and risk assessments of sensitive systems. The agency will enhance its existing continuity of operations plan to include information systems security and submit to the Department of Emergency Management by April 1, 2009. Further, the agency will develop a disaster recovery plan, completing and implementing the security programs in May 2009. Currently, the agency's disaster recovery plan stands at 75% completion.

AGENCY UPDATE:

Management Update (October 2009): Strengthen Information Systems Security Program

Fire Programs completed the Continuity of Operations Plan (COOP) and submitted the document to the Department of Emergency Management in April 2009. During the update of the COOP, Fire Programs ensured that the COOP aligned with the business impact analysis and risk assessments that were completed in February 2009. Fire Programs' COOP is a live document and continues to be updated as needed.

The Disaster Recovery Plan (DRP) was completed in March 2009 as a draft document. Fire Programs' DRP is a live document and continues to be updated as needed. A final version will not be completed until Fire Programs completes the VITA/NG IT Transformation efforts presently underway.

Transformation will allow Northrop Grumman (NG) to manage the infrastructure, providing State agencies with consistent, reliable and measurable services. Transformation projects include desktop refreshes with compatible platforms (completed) and scheduled replacement; network and server modernization and consolidation; enhancement of information security; common messaging; and help desk services.

VITA/NG is navigating the Transformation project. Initial transformation caused failures in Fire Programs' systems that to date have not been remedied and do not meet Fire Programs' business needs. Fire Programs has requested a corrective action workplan from VITA/NG; however, Fire Programs has not received a plan of corrective action at this time.

Complete transformation for Fire Programs is beyond Fire Programs' time scheduling control, being prescribed by VITA/NG scheduling and priorities. Fire Programs' estimate of a realistic completion date is mid-to-late 2011.

Respectfully submitted,

W.G. Shelton, Jr.
Executive Director

COMMONWEALTH of VIRGINIA

Karen Remley, MD, MBA, FAAP
State Health Commissioner

Department of Health
P O BOX 2448
RICHMOND, VA 23218

TTY 7-1-1 OR
1-800-828-1120

November 4, 2009

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

Dear Sir:

We are providing this letter in response to your Report on your Follow-up Review on 2008 Statewide Information Security in the Commonwealth of Virginia, specifically in regards to the two points listed for the Virginia Department of Health (VDH).

Response to recommendations form audit findings from reports issued by the Office of the APA from December 1, 2008 through September 30, 2009.

Update and Expand Security Awareness Training

Response: During the current APA audit of VDH, the auditor was provided documentation showing that employee information Systems security awareness training was provided and documented for all VDH employees. In addition, VDH provided specialized Security Awareness Training for System Owners, Data Owners and System Administrators. VDH understands the importance of training the development staff that supports WebVISION in secure web application coding and has began to search for training to be completed no later than February 28, 2010.

Improve and Test Contingency and Disaster Recovery Planning

Response: During the current APA audit of VDH, the auditor was provided documentation showing Risk Assessments, Business Impact Analysis, Disaster Recovery Planning and testing and Continuation of Operation Plans (COOP) has been completed for all sensitive VDH applications.

Sincerely,

Karen Remley M.D.,M.B.A., FAAP
State Health Commissioner

CC: Goran Gustavsson, Audit Director, APA

COMMONWEALTH of VIRGINIA

SARA REDDING WILSON
DIRECTOR

Department of Human Resource Management

101 N. 14TH STREET
JAMES MONROE BUILDING, 12TH FLOOR
RICHMOND, VIRGINIA 23219
(804) 225-2131
(TTY) 711

TO: Karen Ashby, Auditor, Information Systems Security
Goran Gustavsson, Director, Information Systems Security
Karen Helderman, Director, Information Systems Development

FROM: Sara R. Wilson, DHRM Director Sara R. Wilson

DATE: 4/15/2009

RE: Audit Finding and Recommendation, Improve Information System Security Program

Thank you for the opportunity to respond to your management finding for the Department of Human Resource Management. We have researched the issues in your report and have revised policies and procedures accordingly. Our focus has consistently been on systems security and integrity and, based on your finding, we appreciate the opportunity to strengthen our infrastructure.

Your recommendation to revise the ISO's employee work profile to include the responsibilities required by the Commonwealth policy has been adopted. The Agency ISO will review and evaluate the security program's performance and provide adjustments and training as necessary.

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

(804) 225-2109 FAX (804) 786-3356 TDD (804) 371-8588

COMMONWEALTH of VIRGINIA

MANJU S. GANERIWALA
TREASURER OF VIRGINIA

Department of the Treasury

P. O. BOX 1879
RICHMOND, VIRGINIA 23218-1879
(804) 225-2142
Fax (804) 225-3187

November 4, 2009

Mr. 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 on improvements to Treasury's information security program.

Attached, please find a summary of findings by the Auditor of Public Accounts related to information systems and a current status on each of those items.

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,

Manju Ganeriwala

Manju S. Ganeriwala
State Treasurer

CC: Goran G. Gustavsson, Audit Director
Auditor of Public Accounts

Virginia Department of the Treasury
Update on Fiscal Year 2008 Information Systems-related recommendations

APA Recommendation: Conduct Security Awareness Training Timely

Treasury has not performed security awareness training in accordance with its policies and Commonwealth Standards. Security awareness training provides management some assurance that employees understand their roles and responsibilities for information technology security and allows management to take appropriate action when an employee fails to protect Treasury data and systems.

Treasury is making progress toward implementing a complete security awareness training program by using a web-based system to track completion. This system allows Treasury to ensure that new employees complete training timely and allows them to complete refresher training at least annually.

We recommend that management continue to dedicate the necessary resources to ensure that new and existing employees complete and acknowledge receipt of information technology security awareness training and that records of completed training be retained for at least a three-year period. Additionally, we recommend that Treasury's Information Security Officer ensure that departments are complying with security awareness training requirements by reviewing training content and attendance periodically.

Agency Response: Treasury acknowledges that security awareness training was not performed during the fiscal year-ended June 30, 2008. However, as of July 1, 2008, Treasury hired a new Director of Information Systems and on November 3, 2008, an Information Security Officer was hired. A new security awareness program has been implemented and made available to all employees. All employees had completed the course as of January 10, 2009. Treasury's Information Security Officer ensures that new and existing employees comply with security awareness training and reviews future training content. Records will be kept for three years. New Information Systems policies and procedures were written and approved by management on April 30, 2009 to ensure employees understand their roles and responsibilities for information security.

APA Follow-up Recommendation: Update Risk Assessment and Test Business Continuity Plan

Treasury is in the process of updating their risk assessments and management anticipates updating them by March 2009. Once Treasury has completed their risk assessments, management will have a documented record of present risks to their information systems and the measures taken to minimize those risks.

During fiscal 2008, Treasury did not completely test the business continuity plan as required. Instead, Treasury has only tested components of the plan. By not testing their entire business continuity plan on an annual basis, Treasury cannot evaluate the adequacy and effectiveness of the plan.

Management should complete the risk assessments in a timely manner and test the entire business continuity plan at least annually. As part of this process, Treasury management should review and revise the plan to reflect any concerns noted during testing.

Agency Response: The Risk Assessments for all of Treasury's systems have been completed. The Risk Assessments were reviewed and approved by the IS Steering Committee members and the Agency Head.

The Continuity of Operations Plan (COOP) testing has been approached on an agency-wide and divisional basis. Treasury conducted testing in a manner that is consistent with the COOP objectives and tested the entire plan. Management also completed an in-depth review of the COOP and the plan was revised by streamlining and combining several of the recovery teams with similar functions and making enhancements for ease of use. Training was conducted on the revisions by March 31, 2009.

APA Follow-up Recommendation: Enable Audit Trails and Transaction History on Information Systems

During the prior year, Treasury did not enable audit trails or transaction history features on all of the Department's information technology systems. As a result, individuals could inappropriately change data, either mistakenly or intentionally, and Treasury would not have a readily available mechanism to determine who accessed the data and what activity occurred. For example, during our review, we found one individual with access to change tables within a critical database; this individual was unfamiliar with the tables and lacked the training on how to change the data. Without enabling logging features, Treasury could not easily identify and correct accidentally changed data.

Management is in the process of addressing this concern and procured a log monitoring software tool.

Agency Response: Treasury hired an Information Security Officer on November 3, 2008. Log monitoring software was purchased and implemented in December 2008. Servers and server logs are being monitored daily. Policies and procedures were approved and in effect by April 30, 2009.

COMMONWEALTH of VIRGINIA

Department of Veterans Services

Vincent M. Burgess
Commissioner

Telephone: (804) 786-0286
Fax: (804) 786-0302

November 5, 2009

Goran Gustavsson
Audit Director-Information Systems Security
101 north 14th Street, 8th Floor
Richmond, VA 23219

Dear Mr. Gustavsson;

The Virginia Department of Veterans Services (DVS) appreciates the opportunity to provide an update on the improvements to our information security program.

In the last APA report, the first concern cited was the insufficient staffing for an agency our size. We are happy to report: two new full-time IT positions have been established and hiring has been approved using non-general funds. The hiring and selection process will be completed before December 15, 2009. These new FTEs will report to the Agency IT representative (AITR). These two positions will bring our IT staffing level to three full- time and one part-time employee.

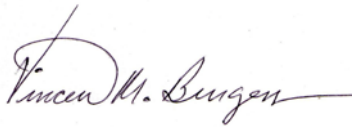
Since the March 24, 2009 audit, which the findings were based on, the DVS has officially appointed an ISO, submitted an IT security audit plan for the next 3 years. That plan is currently being approved by VITA. The DVS is also working on the final stages of an ISO Program and Policy through the Learning Management System (LMS). Our AITR is continuing to work with VITA/NG to clarify the separation of accountability on the requirement under SEC 501 and SAS 70. We expect to have these details resolved during the next 90 days.

The final update we would like to report is to advise we now have the final HIPPA policies and procedures prepared to be circulated for final adoption and implementation. These procedures were developed in conjunction with a HIPPA consultant from the Department of Rehabilitative Services.

I know that our Director of Finance has forwarded comments he received from our AITR, to you earlier today. These comments will provide more detail to what I have noted above.

Thanks for the opportunity to provide this update.

Sincerely,



Vince Burgess

Daniel J. LaVista
Executive Director

COMMONWEALTH of VIRGINIA

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

November 3, 2009

Mr. Walter J. Kucharski
Auditor of Public Accounts
James Monroe Building
101 North 14th Street
Richmond, VA 23219

Dear Walter,

Thank you for the opportunity to comment on the draft report of the first semi-annual Commonwealth Information Security Implementation update. I write to let you know of the progress the State Council of Higher Education for Virginia (SCHEV) has made since the audit of April 2009.

- Thanks in part to the audit finding, SCHEV was able to receive assistance by the two Information Security Officers hired by the Department of Accounts for the purpose of developing a robust information security plan.
- With the assistance of Mr. Edward Miller, SCHEV completed business risk analyses and information security plans for each of the agency's systems.
- We are currently working to finalize the various information security policies for the agency and plan to have these completed by the end of November.
- In the course of the business risk analysis, we have determined that there are a handful of areas where we need to mitigate existing risks and have begun doing so.

With these efforts SCHEV will have a complete Information Security program in place very shortly. I welcome any questions you might have.

Sincerely,

Daniel J. LaVista

COMMONWEALTH of VIRGINIA

George F. Coulter
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

November 4, 2009

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' Commonwealth Information Security Implementation Semi-Annual Update. The review accurately reflects the information security opportunities that have been seized by the Commonwealth, and acknowledges that many opportunities still lie ahead.

We are pleased that the review highlights the significant progress that has been made by the Commonwealth in securing sensitive data. We recognize that small agencies continue to require assistance in developing and sustaining their information security programs. We anticipate that your reviews of small agencies served by the Department of Accounts small agency security outreach effort will demonstrate expected improvements. We will continue to support all Commonwealth agencies and offer guidance as necessary to maintain the trend of improvement in future reviews. As always, we appreciate the professionalism of your staff.

Sincerely,

George F. Coulter

c: The Honorable Len Pomata, Secretary of Technology
John McDonald, Deputy Secretary of Technology
Members, Information Technology Investment Board

Appendix A – Information Security Audit Reports

(December 1, 2008 through September 30, 2009)

Small Agencies *(Position Level less than 100)*					
Agency	**FY 2009 Position Level**	**Last Audit Report Issued**	**Information Security Finding(s) in Last Audit Report**	**Agency has a Security Program that Complies with Best Practices**	**Agency is Following its Security Program**
Board of Accountancy	8	1/20/2009	No	Yes	Yes
Board of Bar Examiners	7	12/16/2008	Yes	No	N/A
Department for the Aging	26	12/10/2008	Yes	No	N/A
Department of Business Assistance	45	4/9/2009	Yes	No	N/A
Department of Fire Programs	74	3/6/2009	Yes	No	N/A
Department of Human Resource Management	94	2/20/2009	Yes	Yes	No
Department of Minority Business Enterprises	28	3/10/2009	Yes	No	N/A
State Board of Elections	17	4/10/2009	Yes	No	N/A
State Council for Higher Education for Virginia	54	3/18/2009	Yes	No	N/A
Virginia College Savings Plan	55	12/12/2008	No	Yes	Yes
Virginia Commission for the Arts	5	8/11/2009	No	Yes	Yes
Virginia Office for Protection and Advocacy	35	4/1/2009	Yes	No	N/A
Virginia State Bar	89	2/27/2009	No	Yes	Yes
			Small Agencies TOTAL	**5 Yes 8 No**	**4 Yes 1 No 8 N/A**

Medium to Large Agencies *(Position Level 100 or above)*					
Agency	**FY 2009 Position Level**	**Last Audit Report Issued**	**Information Security Finding(s) in Last Audit Report**	**Agency has a Security Program that Complies with Best Practices**	**Agency is Following its Security Program**
Attorney General & Department of Law	321	9/16/2009	No	Yes	Yes
Christopher Newport University	787	6/24/2009	Yes	Yes	Yes
College of William and Mary *Including:* • Richard Bland College • Virginia Institute of Marine Science	1,403 112 371	2/12/2009	No	Yes	Yes
Department of Accounts	125	1/12/2009	Yes	Yes	No
Department of Agriculture and Consumer Services *Including:* • Division of Charitable Gaming	526	4/13/2009	Yes	Yes	Yes
Department of Alcoholic Beverage Control	1,048	9/29/2008	Yes	Yes	Yes
Department of Behavioral Health and Developmental Services	9,673	12/10/2008	Yes	Yes	No
Department of Correctional Education	765	4/14/2009	Yes	Yes	Yes
Department of Corrections	12,939	4/22/2009	No	Yes	Yes
Department of Criminal Justice Services	135	1/30/2009	Yes	Yes	No
Department of Emergency Management	138	12/22/2008	Yes	Yes	No
Department of Forestry	320	4/7/2009	Yes	Yes	No
Department of General Services	663	5/8/2009	Yes	Yes	Yes
Department of Health	3,675	12/10/2008	Yes	Yes	No
Department of Health Professions	214	12/10/2008	No	Yes	Yes
Department of Medical Assistance Services	353	12/10/2008	No	Yes	Yes
Department of Mines, Minerals & Energy	234	3/19/2009	Yes	Yes	Yes
Department of Motor Vehicles	2,038	12/12/2008	Yes	Yes	Yes

Agency	FY 2009 Position Level	Last Audit Report Issued	Information Security Finding(s) in Last Audit Report	Agency has a Security Program that Complies with Best Practices	Agency is Following its Security Program
Department of Rehabilitative Services *Including:* • Department for the Deaf and Hard-of-Hearing • Department of the Blind and 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	704 14 164 10 26 190 1,063	12/10/2008	No	Yes	Yes
Department of Social Services	1,662	12/10/2008	No	Yes	Yes
Department of Taxation	997	1/12/2009	Yes	Yes	Yes
Department of the Treasury	121	1/12/2009	Yes	Yes	No
Department of Transportation	8,850	12/12/2008	Yes	Yes	Yes
Department of Veterans Services	609	3/24/2009	Yes	No	N/A
George Mason University	3,465	4/23/2009	No	Yes	Yes
Indigent Defense Commission	540	3/16/2009	Yes	No	N/A
James Madison University	2,835	3/31/2009	No	Yes	Yes
Library of Virginia	208	2/2/2009	No	Yes	Yes
Longwood University	641	5/26/2009	Yes	Yes	Yes
Marine Resources Commission	160	2/26/2009	No	Yes	Yes
Norfolk State University	983	4/24/2009	Yes	Yes	Yes
Old Dominion University	2,283	3/31/2009	No	Yes	Yes
Radford University	1,391	4/14/2009	No	Yes	Yes
State Lottery Department	256	10/1/2009	No	Yes	Yes

Agency	FY 2009 Position Level	Last Audit Report Issued	Information Security Finding(s) in Last Audit Report	Agency has a Security Program that Complies with Best Practices	Agency is Following its Security Program
Supreme Court (Judicial Department) *Excluding:* • Board of Bar Examiners, Indigent Defense Commission, and Virginia State Bar	2,644	5/4/2009	No	Yes	Yes
University of Mary Washington	683	5/4/2009	Yes	Yes	Yes
Virginia Commonwealth University	5,183	12/15/2008	No	Yes	Yes
Virginia Community College System	8,909	9/1/2009	Yes	Yes	Yes
Virginia Employment Commission	865	12/15/2008	No	Yes	Yes
Virginia Military Institute	464	4/13/2009	Yes	Yes	Yes
Virginia State University	771	4/24/2009	Yes	Yes	Yes
Medium to Large Agencies TOTAL				**39 Yes** **2 No**	**32 Yes** **7 No** **2 N/A**
GRAND TOTAL				**44 Yes** **10 No**	**36 Yes** **8 No** **10 N/A**

Appendix B – Next Semi-Annual Update

(October 1, 2009 through March 31, 2010)

The following agencies are included in our Office's work plan for the period October 1, 2009 through March 31, 2010. While the majority of the audit reports for these agencies will be released during this period, some audit reports may be issued after March 31, 2010. In such case, the results of those audit reports will be included in the succeeding Information Security Findings Summary report (April 1, 2010 through September 30, 2010).

College of William and Mary	Frontier Culture Museum of Virginia*
Compensation Board*	George Mason University
Department of Accounts	Gunston Hall*
Department of Alcoholic Beverage Control	Innovative Technology Authority/Center for Innovative Technology*
Department of Aviation*	James Madison University
Department of Behavioral Health and Developmental Services	Jamestown-Yorktown Foundation / Jamestown 2007
Department of Conservation and Recreation	Longwood University
Department of Education	Norfolk State University
Department of Emergency Management	Old Dominion University
Department of Environmental Quality	Radford University
Department of Forensic Science	Science Museum of Virginia*
Department of Game and Inland Fisheries	Southwest Virginia Higher Education Center*
Department of Health	State Corporation Commission
Department of Historic Resources*	University of Virginia
Department of Housing and Community Development	University of Virginia Medical Center
Department of Labor and Industry	Virginia Commonwealth University
Department of Medical Assistance Services	Virginia Economic Development Partnership (Incl. VA Tourism Auth.)*
Department of Military Affairs	Virginia Employment Commission
Department of Motor Vehicles	Virginia Military Institute
Department of Professional and Occupational Regulation	Virginia Museum of Fine Arts
Department of Rail and Public Transportation*	Virginia Museum of Natural History*
Department of Rehabilitative Services	Virginia Polytechnic Institute and State University
Department of Social Services	Virginia Port Authority
Department of State Police	Virginia Racing Commission*
Department of Taxation	Virginia Retirement System
Department of the Treasury	Virginia State University
Department of Transportation	Virginia Workers' Compensation Commission

** Small agency with less than 100 positions*