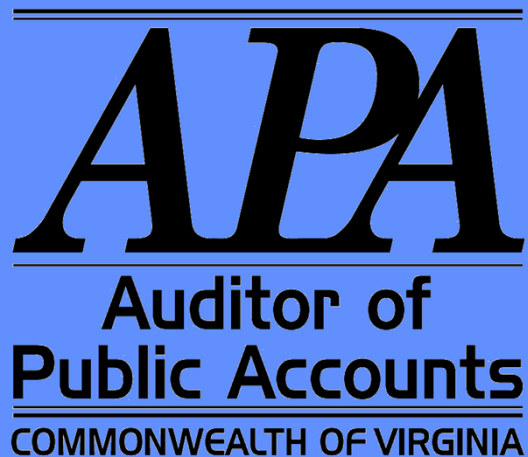


**STATE OF INFORMATION SECURITY
IN THE
COMMONWEALTH OF VIRGINIA
SPRING 2011**

AS OF APRIL 30, 2011



Executive Summary

Overall, agencies and institutions of higher education have adequate information security programs to safeguard confidential and mission critical data. While some agencies need to improve or update their programs to more accurately align with information security standards or to better reflect their current IT environments, only four agencies (3 percent) have inadequate programs where their programs are either out-of-date and not effective, or are missing important sections required by the information security standards.

The remaining 111 agencies (97 percent) have implemented adequate information security programs that follow industry best practices or the Commonwealth's Security Standard SEC 501. While this number by itself is encouraging, we found during the course of our audits that 43 of the 111 agencies (39 percent) need to improve certain sections of their programs in order to fully comply with current best practices and standards.

The most predominant information security issue facing the Commonwealth remains employee computer access controls, followed closely by risk management and contingency plans. Twenty-four (21 percent) of 115 agencies and institutions do not have employee computer access controls that meet the Commonwealth's standards or industry best practice. Twenty-seven (23 percent) do not have risk management or contingency plans that comply with the standards or industry best practice.

The Commonwealth is adequately reviewing and updating the Information Security Standard to ensure compliance with nationally recognized information security standards. The Secretary of Technology on April 4, 2011 approved the last revision of the Commonwealth's information security standard.

– TABLE OF CONTENTS –

| | <u>Pages</u> |
|---|--------------|
| EXECUTIVE SUMMARY | |
| INTRODUCTION | 1 |
| INFORMATION SECURITY SUMMARY | 1-5 |
| Risk Management and Contingency Planning | 3 |
| Essential Security Program Components | 4-5 |
| Other Security Program Requirements | 5 |
| COMMONWEALTH’S INFORMATION SECURITY STANDARD UPDATE PROCESS | 6-7 |
| CONCLUSION | 7 |
| TRANSMITTAL LETTER | 8 |
| AGENCY RESPONSES | 9-12 |
| APPENDIX A: Agency Information Security Program Compliance | 13-17 |
| APPENDIX B: Importance of an Information Security Program | 18 |
| APPENDIX C: Maintaining an Information Security Program | 19 |
| APPENDIX D: Audit Objectives, Scope, and Methodology | 20-21 |

INTRODUCTION

This report is a statewide assessment of information security programs implemented by the Commonwealth's agencies and institutions of higher education, which we issue semi-annually. We conduct security reviews throughout the year during scheduled financial and performance audits of agencies and institutions of higher education.

This report consolidates the information security findings and issues our audits have found in 115 agencies and institutions of higher education. By consolidating this information, we can identify and analyze information security issues facing the Commonwealth across agencies and institutions.

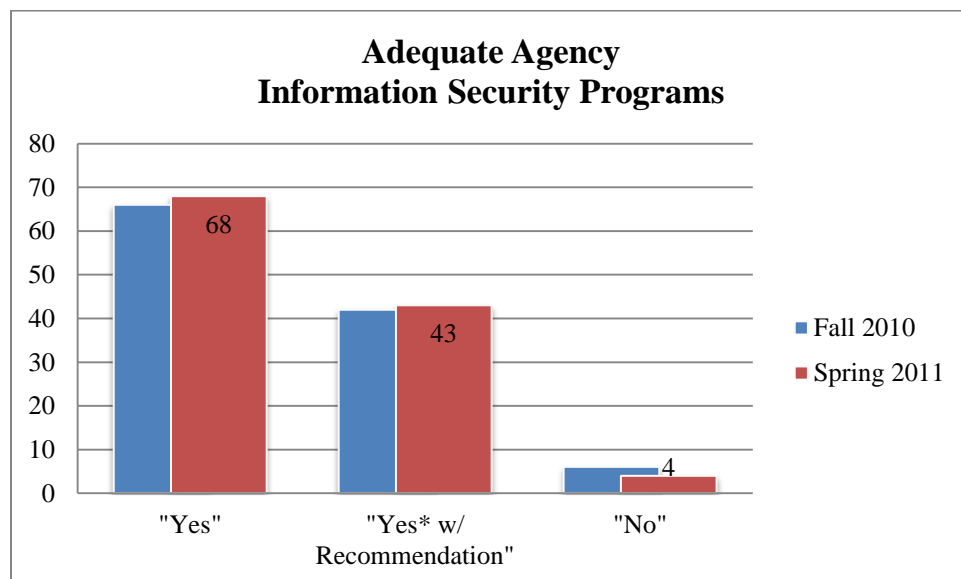
INFORMATION SECURITY SUMMARY

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 of information security programs.

Overall, agencies and institutions of higher education have established adequate information security programs to safeguard confidential and mission critical data.

Our analysis shows that four (three percent) of the 115 entities reviewed do not have adequate information security programs. Compared to the Fall 2010, this is a net improvement of two agencies having moved from not having a program to having a functioning security program.

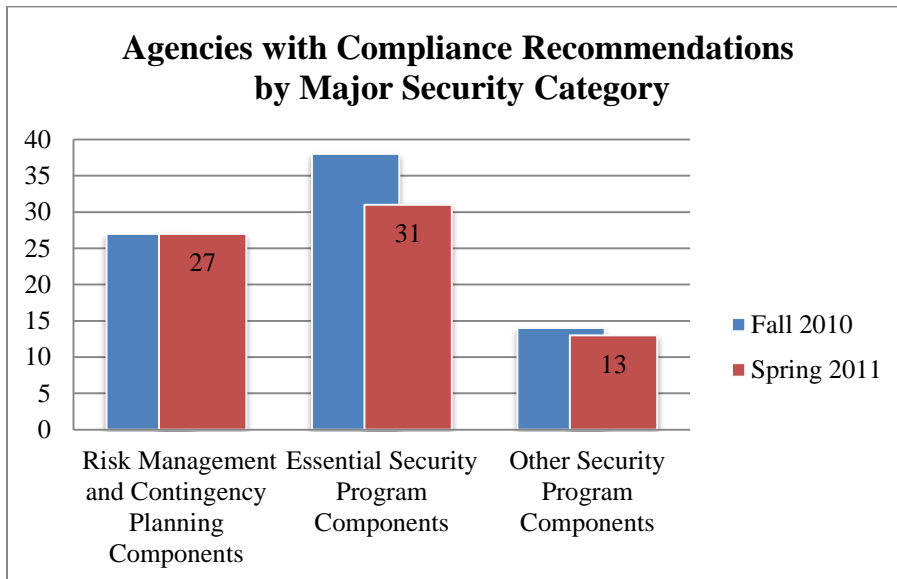


While there has been improvement in the number of agencies and institutions with adequate information security programs, we continue to find areas and issues that these entities need to improve.

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

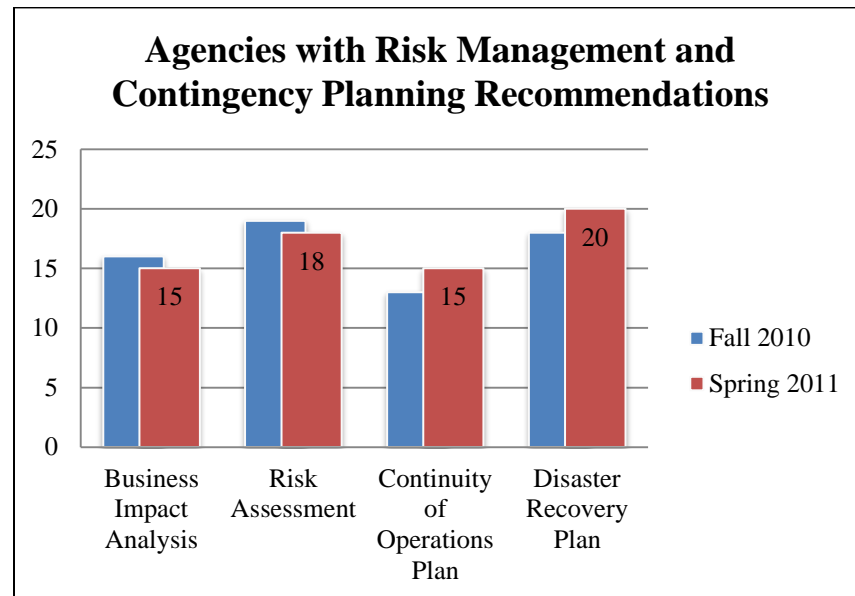
1. *Risk Management and Contingency Planning Components* comprised of the information technology risk assessment, business impact analysis, continuity of operations plan, and disaster recovery plan.
2. *Essential Security Program Components* comprised of seven critical elements of information security that guide or require certain practices designed to mitigate risks and protect mission-critical and confidential data.
3. *Other Security Program 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 issues in the area of risk management and contingency planning (the same as Fall 2010), 31 have issues in essential security program components (seven less than Fall 2010), and 13 have issues in other areas of their security program (one less than Fall 2010).



Risk Management and Contingency Planning

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



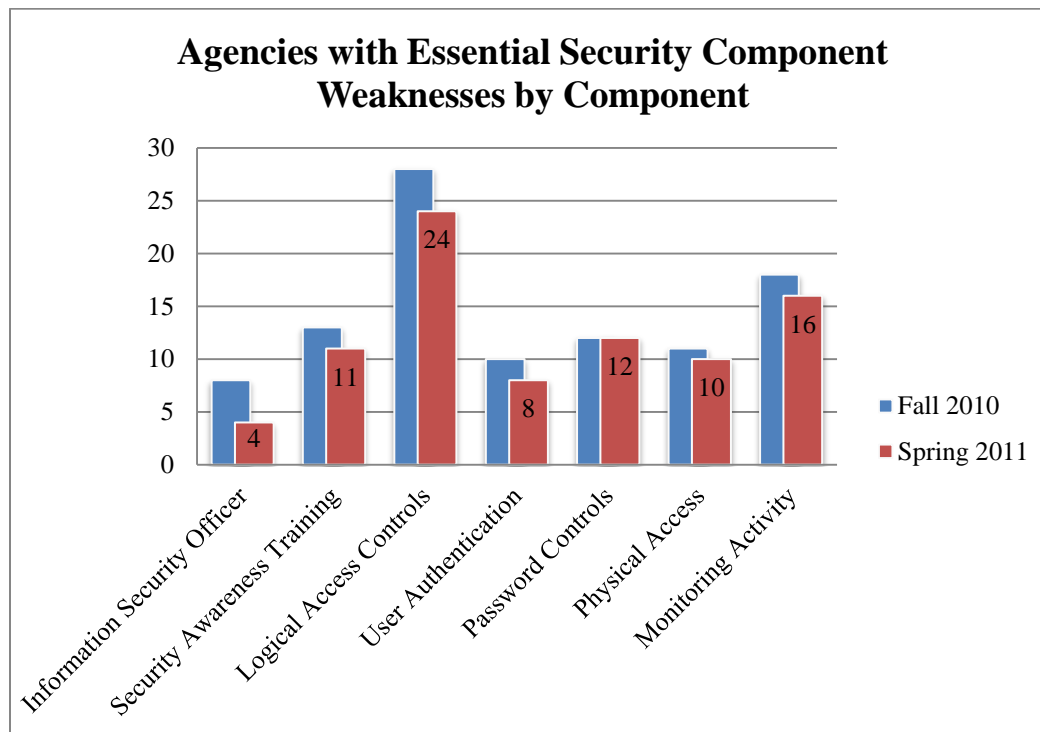
Most agencies and institutions have adequate risk management and contingency plans; 27 (23 percent) have failed to either complete and update these documents, or test these plans. Compared to the Fall 2010 report, this area has remained static. Because agencies and institutions use these plans to determine 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. We found that the weakest component in agencies' and institutions' risk management and contingency plans is the disaster recovery plan. Twenty out of 115 agencies and institutions (17 percent) have incomplete or incorrect disaster recovery plans.

This is a change compared to the Fall 2010 report. In our last report, the primary issue was the risk assessment. Overall, the graph above illustrates that there are less weaknesses in the risk management categories (business impact analysis and risk assessment), and more weaknesses in the contingency categories (the continuity of operations plan and disaster recovery plan). This is an encouraging change, since an agency's risk management categories needs to be in order before the agency can write effective contingency plans. 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 issues 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 24 of 115 agencies and institutions (21 percent) not providing or exercising logical access controls compliant with industry best practices, this is the most problematic component in agencies' and institutions' security programs. However, it is an improvement compared to the Fall 2010 report, when 28 agencies had issues with logical access controls..

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 16 out of 115 agencies and institutions (14 percent) do not comply with the Commonwealth's standards or best practices in monitoring system activity. This is an improvement of two agencies compared to Fall 2010. 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, password controls replaces security awareness training at third place compared to the Fall 2010 report. Agencies and institutions use password controls to ensure a sufficient degree of difficulty for unauthorized users to figure out the passwords used by authorized system users. This includes automatically requiring password complexities, such as using a password with at least one character, one number, one upper case letter, one lower case letter, and a symbol. Twelve out of 115 agencies and institutions (10 percent) do not have password controls that comply with industry best practices.

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, 13 agencies and institutions (11 percent) had issues in these areas. The following is a list of the most common findings 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 agencies and institutions in the Commonwealth are improving their information security programs. Compared to the Fall 2010 report, two agencies have moved from having no security program to having an implemented program. Overall, 111 out of 115 agencies (97 percent) have adequate programs, and 43 of the 111 adequate agencies (39 percent) need improvements or updates to fully meet industry best practices.

COMMONWEALTH'S INFORMATION SECURITY STANDARD UPDATE PROCESS

The Virginia Information Technologies Agency (VITA) is responsible for recommending and developing statewide technical and data policies, standards and guidelines for information technology and related systems, which the Secretary of Technology reviews and approves. The Commonwealth's Information Security Standard is known as the "SEC 501." Unless an agency or institution has an explicit exemption from adhering to this standard, all executive, judicial, and legislative branch agencies must implement policies and procedures that meet the minimum standards in the SEC 501.

The Commonwealth's Information Security Standard is being adequately reviewed and updated to ensure compliance with nationally recognized information security standards.

Since its inception in 2001, VITA has revised the standard six times to keep it updated and aligned with industry best practices. In addition to VITA's continuous internal reviews of this standard to ensure the Commonwealth's compliance with industry best practices, VITA receives feedback and suggestions from several sources, including the Information Security Officer Advisory Group and the Commonwealth Information Security Council.

VITA staff conducts internal reviews of the standard and receives suggestions for changes. When it determines the changes warrant revision, then VITA posts a draft of the revisions on the Online Review and Comment Application (ORCA). The draft stays on ORCA for 30 days; any user of the standard can provide feedback during this period. If the draft contains any requirements that may impact the security controls managed by the Commonwealth's IT infrastructure provider, Northrop Grumman, they also review the draft.

After considering all feedback, VITA staff provides a final draft for consideration by the Chief Information Officer (CIO). The CIO will either recommend the new standard for approval by the Secretary of Technology, or will ask for further review.

The current standard in effect, SEC 501 rev. 6, uses the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISO/IEC 27000 series standards. The ISO 27000 series is one of several information security industry best practices. Two of the other most notable and adopted standards are those published by the National Institute of Standards and Technology (NIST) and the IT Governance Institute (ITGI).

To better align the Commonwealth's standard with the data safeguard requirements of federal information systems and data, VITA is re-aligning SEC 501 to the NIST standards. There are three advantages to making this change.

- 1) The Commonwealth can more easily demonstrate that data protection is the same or better than that required by the federal government for its agencies.

- 2) The NIST information security framework comes with several tools, which VITA, agencies, and institutions can use to ensure compliance. These tools include automated monitoring and baseline information system settings.
- 3) Several commercially available compliance tools already have the NIST standards pre-programmed as a baseline comparison.

VITA has established a project plan that will cover reviewing and analyzing applicability of each of the 18 sections in the NIST standards by the end of the year. VITA anticipates the new Standard for the Commonwealth to be effective as of July 1, 2012, which will give agencies six months to update their policies and procedures.

FINDING #2:

The Virginia Information Technologies Agency (VITA) should continue transforming the Commonwealth's current Information Security Standard, SEC 501, to align with the National Institute of Science and Technology (NIST) standards. This transition will better position agencies to implement the same security controls used by the federal government. The effective date for the new standard is July 1, 2012.

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.

In comparison to our last report issued in the Fall 2010, agencies are improving their information security programs. While five more agencies need to improve compliance with industry best practices, we saw an improvement of two more agencies having moved from having no security program, to having a program.

Agencies and institutions of higher education have also improved their risk management plans compared to the Fall 2010 report. Fewer agencies have issues in risk management plans, and there is a slight increase in agencies with findings in contingency planning. This is the reverse from our finding in our last report, and is an encouraging static as contingency plans are more effective when agencies build them using well developed risk management plans.

Lastly, VITA is updating the Commonwealth's Information Security Standard to align with the standards outlined in industry best practices. VITA is re-aligning the Commonwealth's standard with the same best practices implemented by the federal government. VITA anticipates the effective date of the new standard to be July 1, 2012.



Walter J. Kucharski, Auditor

Commonwealth of Virginia

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

June 21, 2011

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 “**State of Information Security in the Commonwealth of Virginia – Spring 2011**” 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 115 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 June 21, 2011. 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:

Carl E. Garrison, III
State Forester



COMMONWEALTH of VIRGINIA

DEPARTMENT OF FORESTRY

900 Natural Resources Drive, Suite 800

Charlottesville, VA 22903

www.dof.virginia.gov

(434) 977-6555

Fax: (434) 296-2369

June 20, 2011

Mr. Goran Gustavsson, Audit Director
Information Systems Security Specialty Team
101 North 14th Street, 8th Floor
Richmond, VA 23219

Mr. Gustavsson:

Per your June 17, 2011 e-mail, I would like to comment on the progress that DOF has made on the Information Security Plan over the past few months.

The Department of Forestry was without a permanent Director of Information Systems for more than a year from Spring 2009 through Fall 2010 due to the state-wide hiring freeze and did not have the resources to develop and implement an agency Information Security Program. Since November of 2010, the DOF has worked to develop an Information Security Program, and has completed the Risk Assessment and IT Disaster Recovery Plan, a comprehensive Information Security Policy, agency-wide Information Security Awareness Training and very soon an Information Security Audit.

In addition, the DOF will complete an InfoSec Program Audit in June of 2011, and will continue to improve and refine the agency InfoSec program, beginning with a review and update of the DOF policy to match the new Standard and other policies, procedures and guidelines that are under review at this time at VITA.

Thank you for your consideration of this information. If you need anything further, please let me know.

Sincerely,

A handwritten signature in blue ink that reads "Carl E. Garrison III".

Carl E. Garrison, III
State Forester



COMMONWEALTH of VIRGINIA

Virginia Information Technologies Agency

Samuel A. Nixon, Jr.
Chief Information Officer
E-mail: cio@vita.virginia.gov

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

TDD VOICE -TEL. NO.
711

June 28, 2011

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' *Spring 2011 State of Information Security in the Commonwealth of Virginia* report. The report accurately reflects the continued 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.

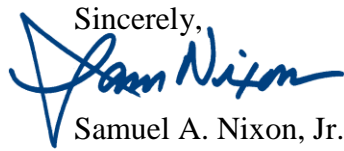
We agree with the first finding of the report that agencies and institutions in the Commonwealth are improving their information security programs. The Virginia Information Technologies Agency (VITA) continues to work in support of agency personnel, and deliver targeted training to them in venues such as the monthly Information Security Officers' Advisory Group meetings and the quarterly Information Security Orientation sessions.

Furthermore, we also agree with the second finding of the report that VITA should continue transforming the Commonwealth's current information security standard, SEC-501, to align with the National Institute of Science and Technology (NIST) standards. The alignment of the current security standard with the NIST security standard 800-53 will provide numerous benefits to the Commonwealth including:

- the ability to easily demonstrate required safeguards by agencies that receive federal funds;
- the availability of both commercial tools and free utilities developed by the federal government, for control management and measurement; and
- the promulgation of a baseline set of associated policies and procedures to be adopted in whole or part by an agency as appropriate.

We are pleased with the continued progress reflected in this report and the confidence expressed in the direction that VITA pursuing with changes to the security standard. As always, we appreciate the professionalism of your staff.

Mr. Walter J. Kucharski
June 28, 2011
Page Two

Sincerely,

Samuel A. Nixon, Jr.

c: The Honorable James D. Duffey, 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 | 2011 Security Program Compliance |
|---|--|---|---|
| Agencies | | | |
| Attorney General and Department of Law | 10/08/2010 | Yes | Yes |
| Board of Accountancy | 03/01/2011 | Yes | Yes |
| Board of Bar Examiners | 12/10/2009 | No | No |
| Center for Innovative Technology | 10/22/2010 | Yes | Yes |
| Commonwealth’s Attorneys’ Services Council | 03/26/2009 | Yes | Yes |
| Compensation Board | 11/17/2010 | Yes | Yes |
| Department for the Aging | 03/15/2011 | Yes* | Yes |
| Department of Accounts - Division of State Internal Auditor | 01/12/2011 | Yes* | Yes |
| Department of Agriculture and Consumer Services - Division of Charitable Gaming | 04/28/2010 | Yes | Yes |
| Department of Alcoholic Beverage Control | 10/18/2010 | Yes* | Yes* |
| Department of Aviation | 12/15/2009 | Yes | 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 Geriatric 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 | 12/14/2010 | Yes* | Yes* |
| Department of Business Assistance | 10/27/2010 | Yes* | Yes* |

| | Audit Report Issue Date | 2010 Security Program Compliance | 2011 Security Program Compliance |
|--|--|---|---|
| Department of Conservation and Recreation | 06/14/2010 | Yes* | Yes* |
| Department of Correctional Education | 04/14/2009 | Yes* | Yes* |
| Department of Corrections - Virginia Parole Board | 05/10/2010 | Yes* | Yes* |
| Department of Criminal Justice Services | 03/26/2010 | Yes | Yes |
| Department of Education | 12/08/2010 | Yes | Yes |
| Department of Emergency Management | 02/16/2011 | Yes | Yes* |
| Department of Employment Dispute Resolution | 01/06/2009 | Yes | Yes |
| Department of Environmental Quality | 05/12/2010 | Yes | Yes |
| Department of Fire Programs | 01/29/2010 | Yes* | Yes* |
| Department of Forensic Science | 06/21/2010 | Yes* | Yes* |
| Department of Forestry | 04/07/2009 | No | No |
| Department of Game and Inland Fisheries | 09/17/2009 | Yes* | Yes* |
| Department of General Services | 05/08/2009 | Yes* | Yes* |
| Department of Health | 12/14/2010 | Yes* | Yes* |
| Department of Health Professions | 12/14/2010 | Yes | Yes |
| Department of Historic Resources | 03/08/2010 | Yes* | Yes* |
| Department of Human Resource Management | 02/20/2009 | Yes* | Yes* |
| Department of Housing and Community Development | 01/12/2011 | Yes | Yes |
| Department of Juvenile Justice | 03/14/2011 | Yes | Yes* |
| Department of Labor and Industry | 10/26/2009 | Yes | Yes |
| Department of Medical Assistance Services | 12/14/2011 | Yes | Yes |
| Department of Military Affairs - Virginia Defense Force | 06/12/2008 | No | Yes |
| Department of Mines, Minerals, and Energy | 03/19/2009 | Yes* | Yes* |
| Department of Minority Business Enterprise | 03/10/2009 | No | Yes* |
| Department of Motor Vehicles | 12/14/2010 | Yes* | Yes* |
| Department of Planning and Budget | 01/13/2011 | Yes | Yes |
| Department of Professional and Occupational Regulation | 10/07/2009 | Yes* | Yes* |
| Department of Rail and Public Transportation | 12/14/2010 | Yes | Yes |
| Department of Rehabilitative Services - Department for the Deaf and Hard-of-Hearing - Department 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 | 12/14/2010 | No | No |
| Department of Social Services | 12/14/2010 | Yes* | Yes* |

| | Audit Report Issue Date | 2010 Security Program Compliance | 2011 Security Program Compliance |
|--|--|---|---|
| Department of State Police | 03/24/2010 | Yes* | Yes* |
| Department of Taxation | 01/13/2011 | Yes* | Yes* |
| Department of the Treasury | 01/13/2011 | Yes | Yes |
| Department of Transportation | 12/14/2010 | Yes | Yes* |
| Department of Veterans Services - Sitter and Barefoot Veterans Care Center - Virginia Veterans Care Center | 03/27/2011 | Yes* | Yes* |
| Frontier Culture Museum of Virginia | 03/23/2010 | Yes | Yes |
| Gunston Hall | 05/10/2010 | Yes | Yes |
| Indigent Defense Commission | 04/01/2010 | Yes* | Yes* |
| Jamestown-Yorktown Foundation / Jamestown 2007 | 05/19/2010 | Yes* | Yes* |
| Library of Virginia | 03/11/2011 | Yes | Yes |
| Marine Resources Commission | 01/19/2011 | Yes | Yes |
| Motor Vehicle Dealer Board | 12/14/2010 | Yes | Yes |
| Office of the Governor and Cabinet Secretaries | 08/12/2010 | Yes | Yes |
| Potomac River Fisheries Commission | 04/12/2010 | Yes | Yes |
| Science Museum of Virginia | 04/23/2010 | Yes | Yes |
| Southwest Virginia Higher Education Center | 06/21/2010 | Yes | Yes |
| State Board of Elections | 01/13/2011 | Yes* | Yes* |
| State Corporation Commission | 10/08/2009 | Yes* | Yes* |
| State Council for Higher Education for Virginia | 03/18/2009 | Yes* | Yes* |
| State Lottery Department | 09/08/2010 | Yes | Yes |
| Supreme Court (Judicial Department) - Court of Appeals of Virginia - Judicial Inquiry and Review Commission - Virginia Criminal Sentencing Commission | 06/10/2010 | Yes* | Yes* |
| Virginia College Savings Plan | 12/08/2010 | Yes | Yes |
| Virginia Commission for the Arts | 08/11/2009 | Yes | Yes |
| Virginia Economic Development Partnership - Virginia National Defense Industrial Authority - Virginia Tourism Authority | 10/21/2009 | Yes | Yes |
| Virginia Employment Commission | 11/15/2010 | Yes* | Yes* |
| Virginia Information Technologies Agency | 07/13/2009 | Yes* | Yes* |
| Virginia Museum of Fine Arts | 04/11/2011 | Yes | Yes |
| Virginia Museum of Natural History | 01/25/2011 | Yes* | Yes* |
| Virginia Office for Protection and Advocacy | 04/01/2009 | No | No |
| Virginia Port Authority | 10/29/2010 | Yes | Yes* |
| Virginia Retirement System | 12/01/2010 | Yes* | Yes |
| Virginia State Bar | 12/10/2010 | Yes | Yes |
| Virginia Workers' Compensation Commission | 11/17/2009 | Yes* | Yes* |

| | Audit Report Issue Date | 2010 Security Program Compliance | 2011 Security Program Compliance |
|--|--|---|---|
| Colleges and Universities | | | |
| Christopher Newport University | 04/29/2011 | Yes* | Yes* |
| College of William and Mary - Richard Bland College - Virginia Institute of Marine Science | 04/14/2011 | Yes | Yes* |
| George Mason University | 02/10/2011 | Yes | Yes |
| James Madison University | 03/26/2010 | Yes | Yes |
| Longwood University | 05/26/2010 | Yes* | Yes* |
| Norfolk State University | 06/17/2010 | Yes* | Yes* |
| Old Dominion University | 03/14/2011 | Yes | Yes* |
| Radford University | 04/22/2011 | Yes | Yes |
| University of Mary Washington | 04/27/2010 | Yes* | Yes* |
| University of Virginia Academic Division - University of Virginia's College at Wise | 10/29/2010 | Yes | Yes |
| University of Virginia Medical Center | 10/29/2010 | Yes | Yes |
| Virginia Commonwealth University | 12/15/2010 | Yes | Yes |
| Virginia Community College System | 06/2011 ^a | Yes | Yes |
| - Blue Ridge Community College | | Yes | Yes |
| - Central Virginia Community College | | Yes | Yes |
| - Dabney S. Lancaster Community College | | Yes* | Yes |
| - Danville Community College | | Yes | Yes |
| - Eastern Shore Community College | | Yes | Yes |
| - Germanna Community College | | Yes | Yes |
| - J. Sargeant Reynolds Community College | | Yes | Yes |
| - John Tyler Community College | | Yes* | Yes |
| - Lord Fairfax Community College | | Yes | Yes |
| - Mountain Empire Community College | | Yes | Yes |
| - New River Community College | | Yes | Yes |
| - Northern Virginia Community College | | Yes* | Yes |
| - Patric Henry Community College | | Yes | Yes |
| - Paul D. Camp Community College | | Yes | Yes |
| - Piedmont Virginia Community College | | Yes | Yes |
| - Rappahannock Community College | | Yes* | Yes |
| - Southside Virginia Community College | | Yes | Yes |
| - Southwest Virginia Community College | | Yes | Yes |
| - Thomas Nelson Community College | | Yes | Yes |
| - Tidewater Community College | | Yes | Yes |
| - Virginia Highlands Community College | | Yes | Yes |
| - Virginia Western Community College | | Yes | Yes |
| - Wytheville Community College | | Yes | Yes |
| Virginia Military Institute | 04/25/2011 | Yes | Yes |

| | Audit Report Issue Date | 2010 Security Program Compliance | 2011 Security Program Compliance |
|---|--|---|---|
| Virginia Polytechnic Institute and State University | 11/04/2011 | Yes | Yes* |
| Virginia State University | 06/23/2010 | Yes* | Yes* |

| | | |
|-------------------------|--------------|--------------|
| Total “Yes” and “Yes*”: | 109 agencies | 111 agencies |
| Total “No”: | 6 agencies | 4 agencies |

Notes:

^a Rating is based on a report that we expect to issue in June 2011.

APPENDIX B: 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.

APPENDIX C: Maintaining 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 life cycle of an information security program.

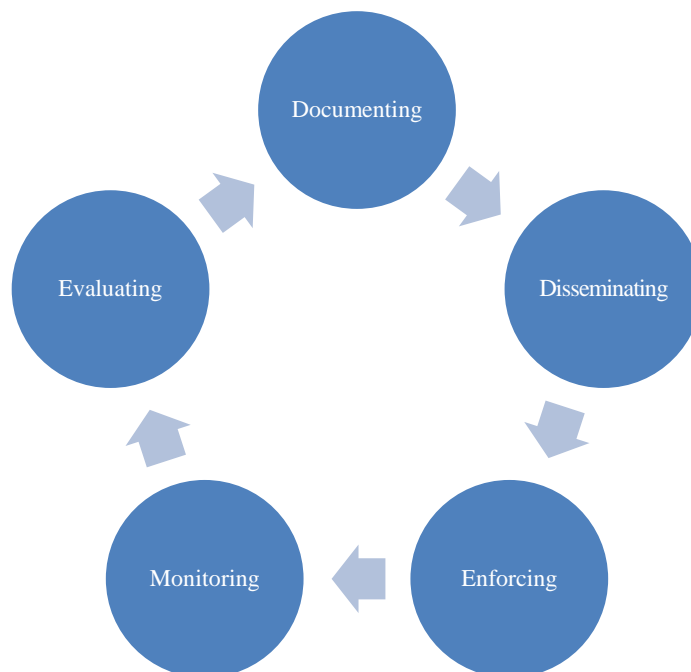


Figure 1. Information Systems Security Program Life Cycle

APPENDIX D: Audit Objectives Scope Maintaining Information Security Program

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) Determine whether that the Commonwealth's Security Standard is updated and compliant with industry best practices.

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 115 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 an agency does not have or has poorly prepared one of these documents, 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 Standard 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. However, having an adequate information security program does not necessarily mean a fully compliant program or no room for improvement to more efficiently and effectively safeguard data. Those agencies with recommendations to improve or enhance programs are indicated with a "Yes*."

Our approach to reviewing the processes to ensure that the Commonwealth is adhering to industry best practices consisted primarily of interviews with VITA staff and examination of current nationally recognized security standards and best practices, including those published by the International Organization for Standardization (ISO), IT Governance Institute (ITGI), and National Institute for Standards and Technology (NIST).