

**2013
STATE OF INFORMATION SECURITY
IN THE
COMMONWEALTH OF VIRGINIA**

**REPORT ON AUDIT
FOR THE PERIOD
JULY 1, 2012 THROUGH JUNE 30, 2013**



Martha S. Mavredes, CPA

Report Highlights

Background Information

The *State of Information Security in the Commonwealth of Virginia* is an annual report that accumulates and analyzes the information security recommendations issued by this office to agencies during audits conducted in the most recent fiscal year.

The statewide analysis allows us to identify the most common information security categories whose controls are not implemented per the Commonwealth's information security standard or agencies' IT policies.

The focus of this statewide review is slightly different from previous statewide reviews. Instead of identifying the number of agencies with inadequate controls in each category across the state, this review focuses on ranking the categories and identifying the most problematic areas.

Key Findings

We reviewed 235 controls in 20 information security categories, which covered 55 agencies in the executive and judicial branches and found the following top-5 inadequate control categories:

- | | |
|--|------------------|
| 1. IT System Data Backup and Restoration | (50% inadequate) |
| 2. Database Security | (44% inadequate) |
| 3. IT Disaster Recovery Plans | (43% inadequate) |
| 4. IT Risk Assessments | (38% inadequate) |
| 5. IT Systems and Data Security (tie) | (33% inadequate) |
| 5. IT Asset Management (tie) | (33% inadequate) |

In total across all categories, 56 out of the 235 controls (24%) did not comply with standards as designed or did not work as required by policy.

We also found that there were no agencies with undocumented information security programs for this review period. This is down from 17 agencies with undocumented programs in our 2006 statewide review. However, while we found documented programs, the quality of these programs vary greatly, which is a contributing factor to the inadequate controls.

Why we did this review

We performed this review to rank and identify inadequately implemented information security controls across the Commonwealth of Virginia.

Scope of this review

Information Security reviews performed at agencies during regularly scheduled financial and performance audits during fiscal year 2013.

235 controls from 20 information security categories were reviewed at 55 agencies.

Information Security Categories Reviewed

- Business Impact Analysis
- Continuity of Operations Plan
- Database Security
- Disaster Recovery Plan
- Firewall Security
- ISO Designation
- IT Asset Management
- IT Security Audits
- IT Security Awareness
- IT System Backup/Restoration
- IT Systems and Data Security
- Logical Access Controls
- Physical Security
- Risk Assessment
- Router Security
- Server Security
- Threat Management
- VPN Security
- Web Application Security

Table of Contents

	Page
Introduction	1-2
Methodology and Scope	3
Top-5 Information Security Weaknesses in the Commonwealth	4-7
Transmittal Letter	8
APPENDIX A – Information Security Control Weaknesses by Category	9-18
APPENDIX B – Agency Responses	19-32

Introduction

The *2013 State of Information Security in the Commonwealth of Virginia* is a statewide assessment of information security programs and controls implemented by the Commonwealth's agencies and institutions of higher education. The purpose of this report is to identify, on a statewide level, the weakest control areas, their impact on securing Citizens' data, and highlight findings.

This report provides a different kind of assessment than we have previously published in our statewide information security reports. Historically, we assessed the adequacy of individual agencies' information security programs and accumulated the findings in each category. Our first report, [Review of Information Security in the Commonwealth of Virginia as of December 1, 2006](#), discovered poorly documented information security programs across agencies.

Since then, there has been an overall downward trend (see Figure 1) of undocumented programs. In our last statewide report, [State of Information Security in the Commonwealth of Virginia – Spring 2011](#), we found that the number of undocumented security programs fell from 17 in 2006 to 4 in 2011. As of last year, 2012, we found that all agencies in-scope to our review have at least a documented program; however, the quality of these programs varies greatly. Some agencies may not meet all requirements set forth by the Commonwealth's Information Security Standards, or by industry best practices, like those published by the National Institute of Standards and Technology (NIST) or Information Systems Audit and Control Association (ISACA), and other agencies operate with outdated security programs due to changes in the organization or IT environment.

Therefore, instead of taking our traditional look at whether individual agencies have documented and implemented programs, we will focus on specific information security program categories and isolate the ones that are the weakest across Commonwealth agencies and those that pose the greatest threat to the Commonwealth's information security posture.

Developing, implementing, and maintaining an information security program is an ongoing task. It is false to assume that once an organization documents and implements a program, that no more work is required. Technology changes at an unprecedented rate and organizational changes to business functions highly affect the way we safeguard mission critical and confidential data.

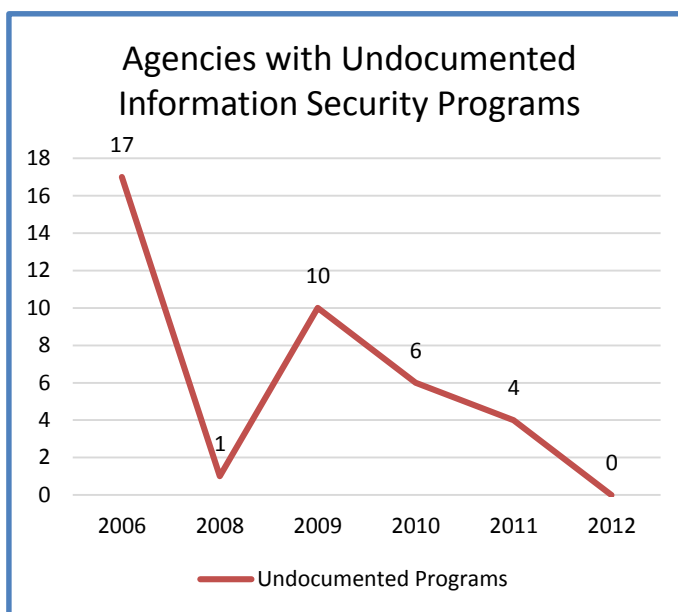


Figure 1: Undocumented Information Security Programs over a six-year period.

Effectively reducing risk to data confidentiality, integrity, and availability requires organizations to keep security programs and the controls they require updated and current. Indeed, investing the effort to develop a program and not keeping it updated is a waste of resources and time. While there is a downward trend in undocumented information security programs in Figure 1, the majority of our agency audit recommendations involve either improving or updating these programs, ensuring appropriate implementation, and providing adequate training.

Methodology and Scope

General IT Security Program Control Categories
<ul style="list-style-type: none">• Information Security Officer Designation• IT Security Awareness and Training• IT Business Impact Analysis• IT Risk Assessment• IT Contingency of Operations Plan• IT Disaster Recovery Plan• IT System Data Backup and Restorations• IT Security Audits• IT Systems and Data Security• Logical Access Controls• IT Physical Security• IT Threat Management• IT Asset Management
Technology-Specific Control Categories
<ul style="list-style-type: none">• Router Security• Wireless Security• Virtual Private Network (VPN) Security• Firewall Security• Server Operating System (O/S) Security• Database Security• Web Application Security

Table 1: Information Security Program and Technology Specific Control Categories.

Through the course of our financial and performance audits, we review the information security categories listed in Table 1, on the left, at each agency. The scope of our reviews depends on several risk factors, including, but not limited to, type and sensitivity of information stored by the agency, current and past agency internal control structure maturity, major changes, and technologies used.

Therefore, the control categories we review across agencies in a fiscal year vary depending on the risk factors associated with the individual agency. This results in different population sizes for each category. For example, we may have reviewed IT Risk Assessments at 16 agencies, whereas we reviewed Wireless Security at three agencies.

To identify the weakest categories in the Commonwealth's security posture, we compared the findings and recommendations this office issued in each category to the total number of reviews we performed in each category during the review period. For example, if we reviewed IT Risk Assessments in 16 agencies and issued IT Risk

Assessment findings to six of those agencies, the result yields a 38 percent exception rate. In other words, 38 percent of the agencies reviewed have inadequate IT Risk Assessments. Based on this methodology, we ranked the control categories from highest to lowest exception rate. The data collected for this summary report reflects our information security findings in our audit reports issued during the period July 1, 2012 through June 30, 2013.

The ranked categories yield the following top five categories that are the most challenging for agencies to keep current or align with security standards.

1. IT System Data Backup and Restoration
2. Database Security
3. Disaster Recovery Plan
4. Risk Assessment
5. IT Systems and Data Security (tie)
5. IT Asset Management (tie)

The next section of this report discusses these Top-5 information security control weaknesses.

Top-5 Information Security Weaknesses in the Commonwealth

The Top-5 information security weaknesses in the Commonwealth are IT System Data Backup and Restoration, Database Security, Disaster Recovery Plan, Risk Assessment, and tied for fifth IT Systems and Data Security and IT Asset Management. We analyze each Top-5 category in the following pages. A full ranking and discussion of all categories are found in Appendix A – Information Security Control Weaknesses in the Commonwealth.

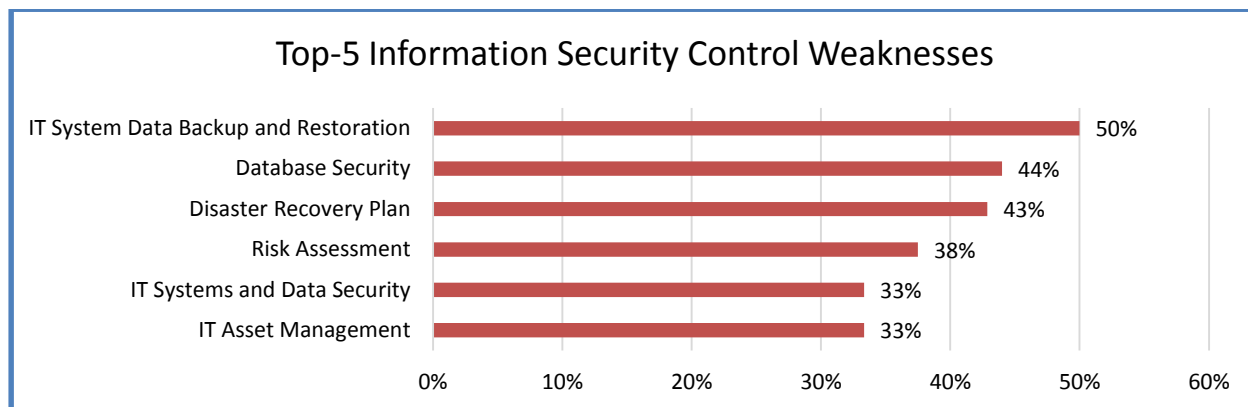


Figure 2: Top-5 Information Security Control Weaknesses.

#1: IT System Data Backup and Restoration

Implemented IT System Data Backup and Restoration plans protect the availability and integrity of the Commonwealth's data. The Disaster Recovery Plans depend on the backup and restoration plans being accurate and verified. Inadequate plans may hinder agencies to restore essential business functions in the event of a disaster, hardware failure, or other unforeseen event.

Issues identified in our audits range from not properly protecting backup media while in transit to not verifying that backups are successful and can be restored.

Three of six agencies tested, or 50 percent, do not have data backup and restoration plans that meet the Commonwealth's information security standard, SEC 501, requirements or industry best practices (Figure 3).

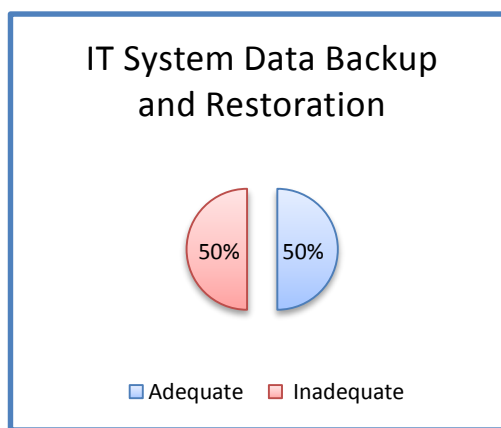


Figure 3: IT System Data Backup & Restoration.

#2: Database Security

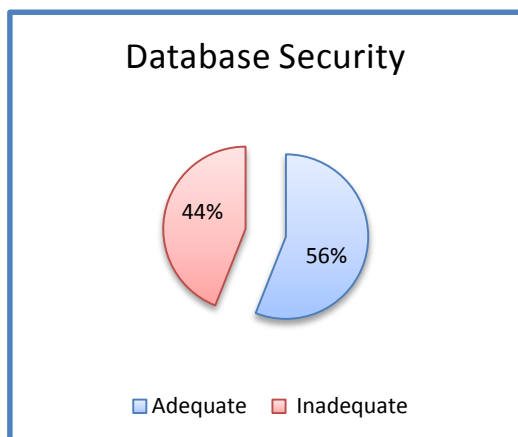


Figure 4: Database Security

Applications often use databases to manage and store data. The most prominent enterprise grade databases in the Commonwealth are Oracle and Microsoft SQL Server. Applications, such as PeopleSoft, Oracle Financials, J.D. Edwards, Banner, and Commonwealth-developed applications use these database platforms. The database management system is one of many security layers that contributes to the general control structure in establishing data confidentiality, integrity, and availability.

The Commonwealth's IT Partnership with Northrop Grumman shares responsibility with the Commonwealth's agencies to maintain and operate these databases for executive branch agencies. However, independent

agencies and institutions of higher education still maintain full operational control over databases.

Our reviews found that agencies that are inadequate in this category do not install or upgrade databases in compliance with the agencies' established policies and procedures. Other agencies lack policies and procedures that include the requirements in the Commonwealth's information security standard or other industry standards.

Eleven of 25 agencies tested, or 44 percent, do not have adequate database security management and configuration practices (Figure 4).

#3: Disaster Recovery Planning Documentation

The Disaster Recovery Plan (DRP) is part of the continuity of operations plan. The DRP identifies the steps necessary to restore IT services that support agencies' essential business functions.

Our reviews found that agencies that are part of the Commonwealth's IT Infrastructure Partnership do not maintain updated disaster recovery plans for systems maintained and operated by the Partnership. While the Partnership is responsible for restoring the files on the system, individual applications that provide specific services require specific and deliberate recovery steps. Agencies in the Partnership are responsible for performing these steps and making the application operational after files are restored.

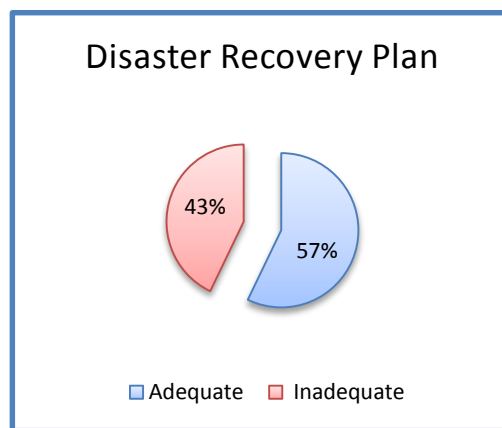


Figure 5: Disaster Recovery Plan

Agencies outside of the Partnership exhibit the same issues, but with the additional responsibility to have a working process to restore files.

Six of 14 agencies tested, or 43 percent, do not have an updated, tested, or accurate disaster recovery plan for IT systems.

#4: Risk Assessment

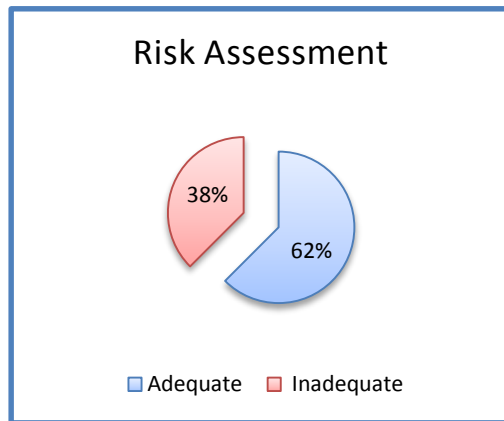


Figure 6: Risk Assessment

The Risk Assessment (RA) requires agencies to evaluate the risks surrounding IT systems containing sensitive data. Agencies must identify potential threats to an IT system and the environment in which it operates, determine the likelihood that threats will materialize, identify and evaluate vulnerabilities, and determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

Our reviews found that agencies do not perform timely updates to their RAs when business functions change or do not perform periodic reviews according to the Commonwealth's information security standard or industry standards.

Six of 16 agencies tested, or 38 percent, do not have an updated or accurate risk assessments.

#5: IT Systems and Data Security

The IT Systems and Data Security category includes several information security controls. Some examples are IT Systems Interoperability, Malicious Code Protection, Application Security, and Wireless Security. These are general controls that serve as layers in securing mission critical and confidential data.

One of three agencies tested, or 33 percent, have weaknesses in one or more of these security layers.

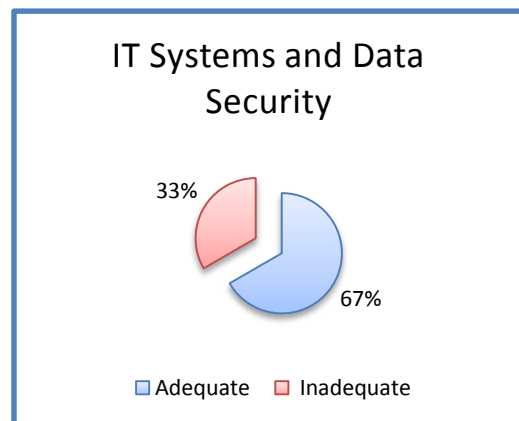


Figure 7: IT Systems and Data Security

#5: IT Asset Management (tie)

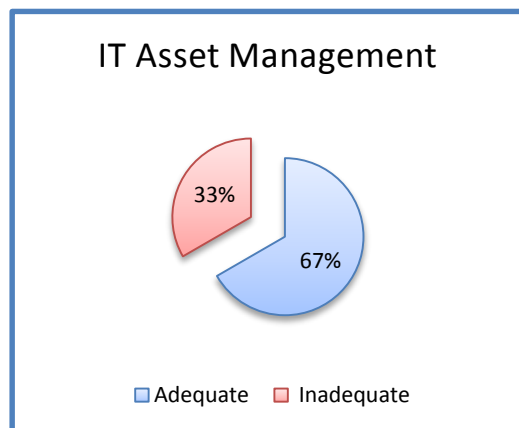


Figure 8: IT Asset Management

IT asset management controls protect IT systems and data by managing the IT assets themselves in a planned, organized, and secure fashion. The controls consist of three main areas; IT asset control, software license management, and configuration management and change control.

The majority of the issues we found concerns configuration management and change controls.

Two of six agencies tested, or 33 percent, do not have adequate IT asset management practices.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 13, 2013

The Honorable Robert F. McDonnell
Governor of Virginia

The Honorable John M. O'Bannon, III
Chairman, Joint Legislative Audit
and Review Commission

We are actively reviewing the Commonwealth's information security controls during our normally scheduled audits and submit our report entitled, "**2013 State of Information Security in the Commonwealth of Virginia**" for your review.

Based on the information security findings in our audit reports published for the period July 1, 2012 through June 30, 2013, this report provides a state-wide perspective that highlights effective and ineffective information security controls throughout the Commonwealth. The report also identifies a list of the Top-5 inadequate controls for the same period.

We intend to continue to review information security controls during our normally scheduled audits and provide annual state-wide reports to summarize any findings.

Agency Responses and Report Distribution

Certain agencies elected to submit current status updates of their Information Security Program implementation progress, which have been included at the end of this report.

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

AUDITOR OF PUBLIC ACCOUNTS

GGG/clj

APPENDIX A – Information Security Control Weaknesses by Category

Through the course of our financial and performance audits, we review the information security categories listed in Table 1, on page 3, at each agency. The scope of our reviews depends on several risk factors, including, but not limited to, type and sensitivity of information stored by the agency, current and past agency internal control structure maturity, major changes, and technologies used.

Therefore, the control categories we review across agencies in a fiscal year vary depending on the risk factors associated with the individual agency. This results in different population sizes for each category. For example, we may have reviewed IT Risk Assessments at 16 agencies, whereas we reviewed Wireless Security at three agencies.

The following bar graph, Figure 9, is a categorized ranking of information security control weaknesses in the Commonwealth of Virginia's agencies and institutions of higher education. This appendix contains additional information the reader may find useful to gain a broader picture of the Commonwealth's information security posture aside from the Top-5 categories discussed in this report.

Additionally, we are providing a table for each control category that delineates the agencies included in the test and whether their control is adequate or inadequate. A link to the audit report is provided for each agency marked as inadequate.

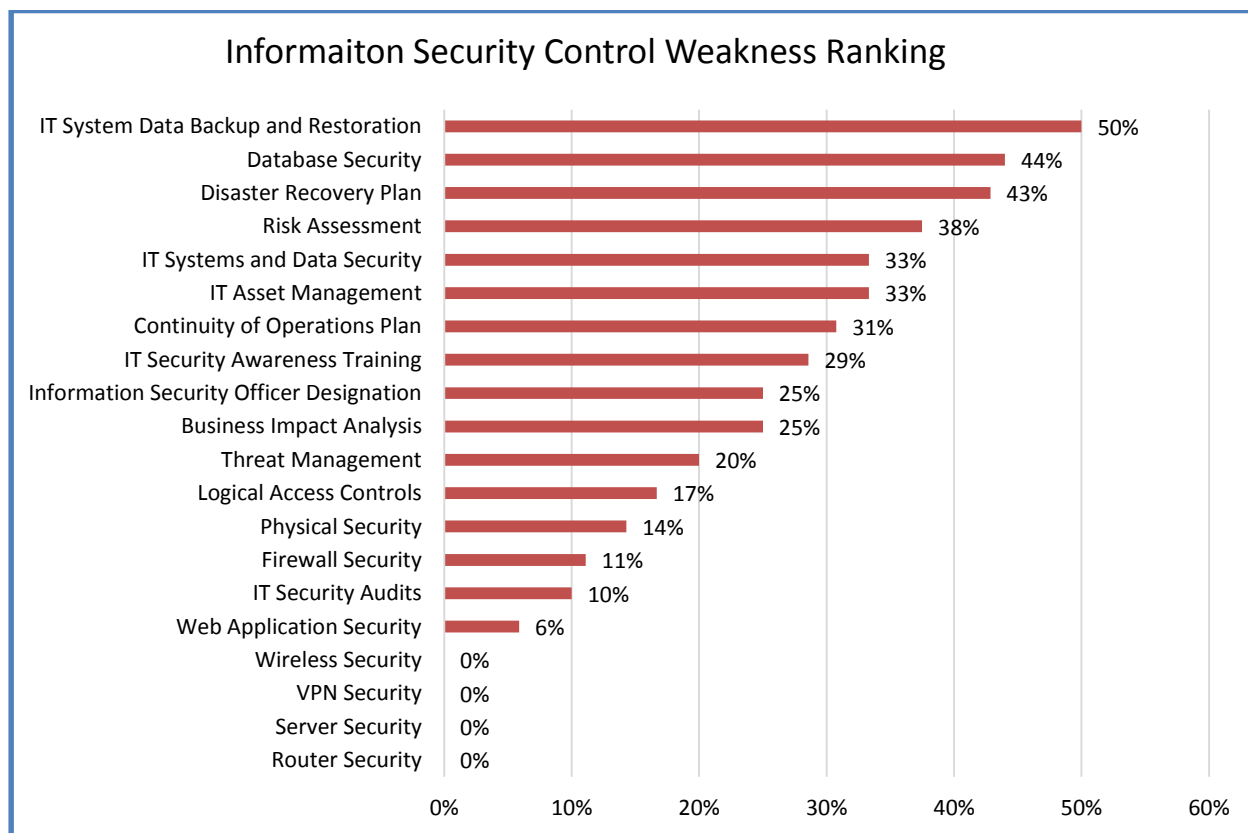


Figure 9: Information Security Control Weakness

#1: IT System Data Backup and Restoration

Our reviews found the following agencies with adequate and inadequate IT System Data Backup and Restoration controls, respectively.

Adequate	Inadequate
Department of Taxation Radford University Virginia Retirement System	Virginia Racing Commission Virginia State Lottery Department Virginia's Judicial System

#2: Database Security

Our reviews found the following agencies with adequate and inadequate Database Security controls, respectively.

Adequate	Inadequate
Christopher Newport University Department of Behavioral Health and Developmental Services Department of Forensic Science Department of Juvenile Justice Radford University University of Virginia Medical Center Virginia College Savings Plan Virginia Commonwealth University Virginia Employment Commission Virginia Retirement System Virginia State Lottery Department Virginia State University Virginia Tech Virginia's Judicial System	Department of Agriculture and Consumer Services Department of Education and Direct Aid to Public Education Department of Health Department of Motor Vehicles Department of Social Services Department of Transportation Longwood University State Corporation Commission University of Virginia Virginia Racing Commission Virginia's Judicial System

#3: Disaster Recovery Planning Documentation

Our reviews found the following agencies with adequate and inadequate Disaster Recovery Planning controls, respectively.

Adequate	Inadequate
Department of Behavioral Health and Developmental Services George Mason University Office of the Attorney General and the Department of Law Virginia Board of Bar Examiners Virginia Department of Emergency Management Services Virginia Information Technologies Agency Virginia Retirement System Virginia State University	Department for Aging and Rehabilitative Services Department of Alcoholic Beverage Control Department of Game and Inland Fisheries Department of Motor Vehicles Department of Social Services Virginia's Judicial System

#4: Risk Assessment

Our reviews found the following agencies with adequate and inadequate Risk Assessment controls, respectively.

Adequate	Inadequate
Department of Accounts Department of Education and Direct Aid to Public Education Department of Forensic Science Department of Game and Inland Fisheries George Mason University Virginia Board of Bar Examiners Virginia Department of Emergency Management Virginia Employment Commission Virginia Information Technologies Agency Virginia Tech	Department for Aging and Rehabilitative Services Department of Alcoholic Beverage Control Office of the Attorney General and the Department of Law State Board of Elections Virginia State Lottery Department Virginia's Judicial System

#5: IT Systems and Data Security (tie)

Our reviews found the following agencies with adequate and inadequate IT Systems and Data Security controls, respectively.

Adequate	Inadequate
Department of Taxation Virginia Employment Commission	Virginia's Judicial System

#5: IT Asset Management (tie)

Our reviews found the following agencies with adequate and inadequate IT Asset Management controls, respectively.

Adequate	Inadequate
Department of Motor Vehicles Department of Taxation Department of Transportation Virginia Retirement System	Department of Social Services Virginia's Judicial System

#7: Continuity of Operations Plan

Agencies develop Continuity of Operations Plans (COOP) to establish a structured approach to continue business operations in case of a disaster, emergency, or unforeseen event. While the document serves as a guide to continue all mission critical operations, it also includes the necessary steps to resume the IT functions that support those operations. Accurate information in the Business Impact Analysis and Risk Assessments is necessary to develop an effective COOP.

Four of 13 (31%) agencies we tested do not have an updated, tested, or accurate continuity of operations plan for IT.

Adequate	Inadequate
Department of Alcoholic Beverage Control Department of Behavioral Health and Developmental Services Department of Game and Inland Fisheries Department of Transportation George Mason University Southern Virginia Higher Education Center Virginia Board of Bar Examiners Virginia Department of Emergency Management Virginia Information Technologies Agency	Department for Aging and Rehabilitative Services Department of Motor Vehicles Office of the Attorney General and the Department of Law Virginia's Judicial System

#8: IT Security Awareness and Training

The IT Security Awareness and Training programs need to provide IT system managers, administrators, users, and contractors with awareness of system security requirements and of their responsibilities to protect IT systems and data.

Four of 14 (29%) agencies we tested do not have adequate security awareness programs.

Adequate	Inadequate
Department of Accounts Department of Behavioral Health and Developmental Services Department of General Services Department of Motor Vehicles Department of the Treasury George Mason University The College of William and Mary Virginia Commonwealth University Virginia Department of Emergency Management Virginia Military Institute	Department for Aging and Rehabilitative Services Department of Education and Direct Aid to Public Education Department of Game and Inland Fisheries Virginia's Judicial System

#9: Information Security Officer Designation (tie)

The Information Security Officer (ISO) is responsible for developing and managing the agency's information security program in accordance with the Commonwealth's information security standard, SEC501, and industry standards and best practices.

One of four (25%) agencies we tested has not adequately designated the agency ISO with appropriate authority.

Adequate	Inadequate
Department of Game and Inland Fisheries Department of General Services Virginia Board of Accountancy	Virginia's Judicial System

#9: Business Impact Analysis (tie)

The Business Impact Analysis (BIA) identifies agencies' business functions and highlights those that are essential to the agency's mission. The BIA also identifies the resources required to support these essential functions. An updated and accurate BIA is necessary to ensure that essential business functions have the appropriate safeguards that consider data confidentiality, integrity, and availability.

Four of 16 (25%) agencies we tested do not have an updated or accurate business impact analysis.

Adequate	Inadequate
Department of Alcoholic Beverage Control Department of Forensic Science Department of Rehabilitative Services including Woodrow Wilson Rehabilitation Center George Mason University Office of the Attorney General and the Department of Law Old Dominion University University of Virginia Virginia Board of Bar Examiners Virginia Department of Emergency Management Virginia Employment Commission Virginia Information Technologies Agency Virginia State Lottery Department	Department of Game and Inland Fisheries Department of Health State Board of Elections Virginia's Judicial System

#11: Threat Management

Threat management protects IT systems and data by preparing for and responding to information security incidents. Threat management consists of four main categories; threat detection, monitoring and logging, incident handling, and data breach notification.

One of five (20%) agencies does not have adequate threat management practices to detect, prevent, or properly respond to a security incident.

Adequate	Inadequate
Department of Motor Vehicles Department of Social Services Department of Taxation Department of Transportation	Virginia's Judicial System

#12: Logical Access Controls

Logical access controls protect IT systems and data by verifying and validating that users are who they say they are and that they are permitted to use the IT systems and data they are attempting to access. Users are accountable for any activity on the system performed with the use of their

account. Logical access controls also include account management, password management, and remote access.

Some of the most common issues include insufficient account reviews, poor separation of duties, and accounts remaining active for terminated employees.

Nine of 54 (17%) agencies do not have adequate logical access controls.

Adequate	Inadequate
<p>Department of Agriculture and Consumer Services</p> <p>Department of Alcoholic Beverage Control</p> <p>Department of Aviation</p> <p>Department of Behavioral Health and Developmental Services</p> <p>Department of Education</p> <p>Department of Forensic Science</p> <p>Department of Health</p> <p>Department of Health Professions</p> <p>Department of Juvenile Justice</p> <p>Department of Medical Assistance Services</p> <p>Department of Rail and Public Transportation</p> <p>Department of Social Services</p> <p>Department of Taxation</p> <p>Department of the Treasury</p> <p>Department of Transportation</p> <p>Frontier Culture Museum of Virginia</p> <p>George Mason University</p> <p>Gunston Hall</p> <p>James Madison University</p> <p>Longwood University</p> <p>Office of the Attorney General and the Department of Law</p> <p>Old Dominion University</p> <p>Radford University</p> <p>Science Museum of Virginia</p> <p>State Board of Elections</p> <p>State Corporation Commission</p> <p>The College of William and Mary</p> <p>University of Mary Washington</p> <p>University of Virginia</p> <p>University of Virginia Medical Center</p> <p>Virginia Board of Accountancy</p> <p>Virginia Board of Bar Examiners</p> <p>Virginia College Savings Plan</p> <p>Virginia Commonwealth University</p> <p>Virginia Employment Commission</p> <p>Virginia Information Technologies Agency</p> <p>Virginia Military Institute</p> <p>Virginia Museum of Fine Arts</p>	<p>Christopher Newport University</p> <p>Department for Aging and Rehabilitative Services</p> <p>Department of Accounts</p> <p>Department of Game and Inland Fisheries</p> <p>Department of General Services</p> <p>Department of Motor Vehicles</p> <p>Jamestown-Yorktown Foundation</p> <p>Virginia Department of Emergency Management</p> <p>Virginia's Judicial System</p>

Adequate (cont'd)	Inadequate (cont'd)
Virginia Museum of Natural History Virginia Racing Commission Virginia Retirement System Virginia State Bar Virginia State Lottery Department Virginia State University Virginia Tech	

#13: Physical Security

Physical security safeguards facilities that house IT equipment, systems, services, and personnel. These safeguards include specific minimum requirements for agencies that house their own data centers.

Most of the weaknesses relate to undocumented policies and procedures. Overall, agencies have implemented adequate controls; however, some agencies lack documented policies and procedures that agencies can use to ensure consistent implementation.

One of seven (14%) agencies does not meet the minimum physical security requirements in the Commonwealth's information security standard.

Adequate	Inadequate
Department of Behavioral Health and Developmental Services Department of the Treasury Department of Transportation The College of William and Mary Virginia Military Institute Virginia Retirement System	Virginia's Judicial System

#14: Firewall Security

Firewalls protect private networks from public visibility and serve as a general control security layer. Typically, organizations separate internal private networks from public networks, such as the Internet, by writing rules in the firewall that dictate which network traffic can pass and which cannot. While the Commonwealth's IT Partnership with Northrop Grumman maintains and operates these devices for executive branch agencies, independent agencies and institutions of higher education still maintain operational control over these devices.

One of nine (11%) agencies does not have adequate firewall security management and configuration practices.

Adequate	Inadequate
George Mason University Longwood University State Corporation Commission The College of William and Mary	Virginia State Lottery Department

Adequate (cont'd)	Inadequate (cont'd)
University of Virginia Virginia Retirement System Virginia State Bar Virginia's Judicial System	

#15: IT Security Audit Plans

IT Security Audits assess whether implemented IT security controls properly mitigate risk and that these controls are adequate and effective. Agencies are responsible for developing a three year plan that covers a review of IT security controls over each sensitive IT system.

One of ten (10%) agencies does not have a plan that coordinates IT Security Audits and ensures sufficient coverage over a 3-year period.

Adequate	Inadequate
Department of Accounts Department of General Services Department of Health Department of Motor Vehicles Department of Social Services Department of Taxation Department of Transportation Office of the Attorney General and the Department of Law Virginia State University	Department of the Treasury

#16: Web Application Security

An increasing number of applications interact with users through a web browser interface. Some applications are accessible to citizens through the internet and others are for employee use only and accessible only on internal agency networks. In either scenario, a properly configured web application is very important to maintain appropriate safeguards over sensitive data. For web applications that face the internet, these safeguards need to be even stronger. Agencies create, maintain, and operate web applications.

One in 17 (6%) agencies has not designed their web applications according to industry best practice guidelines.

Adequate	Inadequate
Christopher Newport University Department of Alcoholic Beverage Control Department of Health Department of Juvenile Justice Department of Taxation Longwood University Old Dominion University Radford University	Department of Motor Vehicles

Adequate (cont'd)	Inadequate (cont'd)
University of Mary Washington University of Virginia University of Virginia Medical Center Virginia College Savings Plan Virginia Commonwealth University Virginia Employment Commission Virginia Military Institute Virginia State Lottery Department	

#17: Wireless Security (tie)

Wireless access points (WAPs) allow mobile users to connect to public and private networks. While allowing mobile users to connect to public networks present relatively low risk, allowing wireless connections to private networks presents a significantly higher risk. Improperly configured or controlled WAPs may circumvent security controls designed to protect sensitive data. While the Commonwealth's IT Partnership with Northrop Grumman maintains and operates these devices for executive branch agencies, independent agencies and institutions of higher education still maintain operational control over these devices.

All three agencies that maintain WAPs outside the IT Partnership and that we tested during this period have properly configured WAPs.

Adequate	Inadequate
Department of Alcoholic Beverage Control Radford University University of Virginia	

#17: VPN Security (tie)

Virtual Private Networks (VPNs) allow mobile and remote users to connect securely via strong encryption to the office or to a specific IT system containing sensitive data. While the Commonwealth's IT Partnership with Northrop Grumman maintains and operates these devices for executive branch agencies, independent agencies and institutions of higher education still maintain operational control over these devices.

All three agencies we tested have adequate VPN security management and configuration practices.

Adequate	Inadequate
George Mason University Virginia Commonwealth University Virginia Military Institute	

#17: Server Security (tie)

The server operating system is necessary to run databases, such as Oracle, and applications, such as PeopleSoft. Without an operating system, databases and applications do not know how to, for

example, communicate with other computers or how to store information on computer memory devices. The server operating system is a “defense in-depth” layer that contributes to the general control structure in establishing data confidentiality, integrity, and availability. While the Commonwealth’s IT Partnership with Northrop Grumman maintains and operates these servers for executive branch agencies, independent agencies and institutions of higher education still maintain operational control over these devices.

All six agencies tested have adequate Server Security management and configuration practices.

Adequate	Inadequate
Department of Alcoholic Beverage Control George Mason University Old Dominion University University of Mary Washington University of Virginia Virginia Tech	

#17: Router Security (tie)

A router is a device that ties networks together. The Commonwealth uses these devices to connect agency networks together and ultimately to connect to the internet. Improperly configured routers increase the risk of potential attackers to penetrate into agencies’ private networks. While the Commonwealth’s IT Partnership with Northrop Grumman maintains and operates these devices for executive branch agencies, independent agencies and institutions of higher education still maintain operational control over these devices.

All four agencies outside the IT Partnership umbrella we tested during this period have properly managed and configured their routers.

Adequate	Inadequate
Christopher Newport University Longwood University Virginia State University Virginia’s Judicial System	



September 30, 2013

Ms. Martha S. Mavredes
Auditor of Public Accounts
P. O. Box 1295
Richmond, VA 23218

Dear Ms. Mavredes:

Related to the 2013 State of Information Security in the Commonwealth of Virginia, Appendix A number 12 (Logical Access Controls), we offer the following response and request its addition within Appendix B of your final report.

At the time of the finding, Christopher Newport University was not in full compliance with Commonwealth Logical Access Control measures, although there was adequate protection to alleviate the threat of a breach, which included two-factor authentication. As of the 1st of June, 2013, the university has implemented measures to ensure full compliance with the requirements of the Security Standard.

This work was completed by Information Technology Services with oversight and accountability by the Chief Information Officer.

Sincerely,

A handwritten signature in black ink, appearing to read 'William L. Brauer', followed by a horizontal line.

William L. Brauer,
Executive Vice President



COMMONWEALTH OF VIRGINIA
DEPARTMENT FOR AGING AND REHABILITATIVE SERVICES

JAMES A. ROTHROCK
Commissioner

8004 Franklin Farms Drive
Henrico, VA 23229

Office (804) 662-7000
Toll free (800) 552-5019
TTY Toll free (800) 464-9950
Fax (804) 662-9532

September 27, 2013

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

Mr. Gustavsson:

Per your September 23, 2013 e-mail, I would like to comment on the progress that the Department for Aging and Rehabilitative Services (DARS) has made on the Information Security Plan over the past few months.

DARS Information Security Program was cited for non-compliance in several areas including Risk Assessments, Disaster Recovery Planning, Continuity of Operations Planning, Security Awareness Training, and Logical Access Controls. We have known of these deficiencies and have actively engaged in implementing corrective action plans.

Currently seven of eight risk assessments are complete. We are planning our disaster recovery strategy that has two parts; a portfolio of screen shots to collect data on paper and alternate servers in an alternate location. We are working with VITA to have these servers placed into production. Beginning in fiscal year 14, we are funding additional risk manager resources to improve the synchronization between our VDEM based COOP plan and COOP requirements of VITA.

Security Awareness Training was provided and encouraged across DARS beginning this past May 2013. To date a large majority of computer users have completed the training. The curriculum is being expanded to address security standards related to Personally Identifiable Information (PII). A final area of inadequate compliance is logical access controls for two of our agency applications. For each of these applications, Code development is required and the necessary effort is underway to be completed in the Winter of 2013-14.

We believe our due diligence will result in significantly greater compliance levels in our upcoming audits. Thank you for your consideration of this information. If you need anything further, please let me know.

Sincerely,


James A. Rothrock

20

JAR/es



COMMONWEALTH of VIRGINIA

Department of Game and Inland Fisheries

Douglas W. Domenech
Secretary of Natural Resources

Robert W. Duncan
Executive Director

September 27, 2013

Martha S. Mavredes, CPA
Auditor of Public Accounts
James Monroe Building
101 North 14th Street 8th Floor
Richmond, VA 23219

Dear Ms. Mavredes:

Thank you for this opportunity to respond to the findings of the *2013 State of Information Security in the Commonwealth of Virginia*. We take information security seriously and are pleased to report on all four findings of inadequacy for the Department of Game and Inland Fisheries:

- #3: Inadequate Disaster Recovery Planning Documentation
 - ✓ We now have a comprehensive disaster recovery plan and we completed a table top exercise of our plan earlier this year.
- #8: Inadequate IT Security Awareness and Training
 - ✓ We now have security awareness training not only for our end users, but also for developers, system owners and data owners. The first annual training is complete.
- #9: Inadequate Business Impact Analysis
 - ✓ We now have a BIA that was developed within SEC 501 requirements that is much more comprehensive than the agency's previous BIA.
- #12: Inadequate Logical Access Controls
 - ✓ We now immediately revoke user privileges upon a reported change or departure. We have reviewed the entire current user list and verified each and every privilege as valid and current.

Department personnel made considerable strides to rectify weaknesses found in the agency's IT systems. Not only do we strive to meet state requirements, we too think it is important to safeguard the public who entrusted their information to the agency. Thank you for the review and your support as we addressed the issues identified.

Sincerely,

A handwritten signature in blue ink that reads "Robert W. Duncan".

Robert W. Duncan
Executive Director

RWD/ag

21



COMMONWEALTH of VIRGINIA

Department of Motor Vehicles
2300 West Broad Street

Richard D. Holcomb
Commissioner

Post Office Box 27412
Richmond, VA 23269-0001

September 27, 2013

Ms. Martha S. Mavredes
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218

Subject: 2013 State of Information Security in the Commonwealth of Virginia DRAFT

Dear Ms. Mavredes:

The Virginia Department of Motor Vehicles (DMV) appreciates the opportunity to respond to the *2013 State of Information Security in the Commonwealth of Virginia* report.

The inadequacies identified in the report are the result of the 2012 APA Audit, i.e. the prior year's audit. On receiving the 2012 Audit Report, DMV prepared a detailed Corrective Action Plan (CAP) and has been diligently following it to remediate the identified issues.

As part of the remediation, DMV has contracted with an individual with the necessary skills and experience to provide an additional resource in the IT Security Office. This is allowing DMV to better implement the CAP.

The APA has recently completed the 2013 Audit and is reviewing the auditor's work. An evaluation of the remediation work for the prior year will be included in the final report. As of this date, DMV anticipates the release of the report soon and continues to proceed with all necessary remediation.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard D. Holcomb", written over a large, stylized capital "T" that serves as a signature element.

Richard D. Holcomb

RDH:db



COMMONWEALTH of VIRGINIA

DAVID A. VON MOLL, CPA
COMPTROLLER

Office of the Comptroller

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

September 24, 2013

Ms. Martha S. Mavredes
Auditor of Public Accounts
James Monroe Building
101 N. 14th Street
Richmond, Virginia 23219

Dear Ms. Mavredes:

The Department of Accounts (Accounts) appreciates the opportunity to respond to the 2013 State of Information Security in the Commonwealth of Virginia Audit Report. We give your comments the highest level of importance and consideration as we continue to review and improve our current practices.

Comments to Management

Enhance Controls Over System Access for Critical Systems

Accounts understands the risks associated with granting Accounts' employees system access to CIPPS and CARS. Accounts plans to document the policies and procedures for granting access to both CIPPS and CARS, addressing the type of access necessary to accomplish specific job functions that are unique to Accounts. Accounts currently has in place a semi-annual review of CARS Security for staff and plans to extend this process to CIPPS Security. Accounts will also include CIPPS Security in our internal control testing pursuant to ARMICS. As noted in our discussions, Accounts is responsible for unique and significant mission critical functions that comport directly to the Commonwealth's overall financial management goals and objectives. This critical responsibility necessitates certain key and experienced staff members maintain specific security capabilities that may appear to be outside of their normal duties to ensure these functions are executed in a timely and accurate manner. Accounts' management will continue to monitor these circumstances and use prudent judgment to ensure security capabilities granted are appropriate and necessary. Accounts recognizes the importance of training staff responsible for granting CIPPS system access and will ensure adequate training is provided.

Sincerely,

David A. Von Moll

Copy: Lewis R. McCabe, Jr., Assistant State Comptroller – Accounting & Reporting



COMMONWEALTH of VIRGINIA

Patricia I. Wright, Ed.D.
Superintendent of Public Instruction

DEPARTMENT OF EDUCATION
P.O. BOX 2120
Richmond, Virginia 23218-2120

Office: (804) 225-2023
Fax: (804) 371-2099

September 27, 2013

Ms. Martha S. Mavredes
Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

The Department of Education has made significant progress in correcting the findings included in the *2013 State of Information Security* in the Commonwealth of Virginia draft report, and we are providing the following agency response to be included in Appendix B of the report.

Page Number	Finding Contained in Current DRAFT Information Security Report	Department of Education Response
11	#2: Database Security Our reviews found the following agencies with adequate and inadequate Database Security controls, respectively.	<u>Audit finding from 2011</u> - Logical Access: Implement changes to the SSWS Account Management process to bring the system into compliance with the Commonwealth of Virginia Information Technology Security Standards that apply to Logical Access Controls. <u>Corrective Action Items</u> : Several security changes to the Department's Single Sign-on Web System (SSWS) portal have been implemented. Users were prompted to answer seven of twenty-five security questions. These questions are now used to unblock accounts if a password has been entered incorrectly three times or the account becomes blocked due to lack of use.

Page Number	Finding Contained in Current DRAFT Information Security Report	Department of Education Response
		<p>Password and account aging has been implemented. As the time for a required password change approaches, within five days, the account holder is given a reminder message at each log in. The system automatically assigns a temporary password to accounts where the user has not conformed to the security requirement (has not changed password within seven days after crossing ninety day threshold). If the temporary password is not changed within seven days, the account becomes blocked and a security question must be answered. If the password is not changed within one hundred eighty days, the account is deactivated. If the password is still not changed within three hundred sixty-five days, the account is deleted. E-mail notifications are sent to the account holder as each of these events occur and e-mail notifications are sent to the account holder's local SSWS Account Manager for deactivation and elimination.</p> <p>VDOE has developed more detailed descriptions of the roles assigned to users and used in the semi-annual review access by application owners. The descriptions are now in the production environment and the process requires the requester to read the role descriptions before selecting a role for the employee.</p> <p>VDOE has created an SSWS-based application to centrally manage security related information regarding contractors. System training for staff occurred September 16, 2013. The</p>

Page Number	Finding Contained in Current DRAFT Information Security Report	Department of Education Response
		<p>system went live September 23, 2013, allowing verification that contractors do not have access to VDOE systems upon termination of their employment. VDOE added contractor access to VDOE systems in CY 2012 4Q as an item reviewed annually as part of the agency ARMICS process.</p>
13	<p>#8: IT Security Awareness and Training The IT Security Awareness and Training programs need to provide IT system managers, administrators, users, and contractors with awareness of system security requirements and of their responsibilities to protect IT systems and data.</p> <p>Four of 14 (29%) agencies we tested do not have adequate security awareness programs.</p>	<p><u>Audit finding from 2010</u> - Personnel Security: Information Security Awareness and Training: Information Technology (IT) Security Awareness Training Does Not Include All Required Topics or Address All Required Audiences.</p> <p><u>Corrective Action Items:</u></p> <p>Contractors are now included in yearly security training through the Knowledge Center.</p> <p>Delivery methods for the IT role-based security training program have been reviewed. In addition to the FERPA and Cyber Security Awareness training provided to all VDOE users, additional role-based courses given to specific users through the Knowledge Center include: Systems Security Planning, IT Systems Hardening, and Data Protection and Sensitivity Analysis.</p> <p>A system was implemented in Q2 within the agency's enterprise system, SSWS, for a required annual review and acceptance by all VDOE system users of three policies related to the agency's information technology: Acceptable Use, Information Security, and the</p>

Page Number	Finding Contained in Current DRAFT Information Security Report	Department of Education Response
		agency-specific Family Educational Rights and Privacy Act (FERPA) policies. The system allows employees to annually review these VDOE security policies, and certify that they have read and accept the terms to allow for logging, tracking and reminders—all for efficient compliance. The next review will occur January 2014 and annually in January thereafter.

Please contact Kent Dickey, Deputy Superintendent for Finance and Operations, at 804-225-2025, if additional information is needed.

Sincerely,



Patricia I. Wright, Ed.D.
Superintendent of Public Instruction

PIW/KCD/cle

LONGWOOD
UNIVERSITY

201 High Street
Farmville, Virginia 23909
tel: 434.395.2001
fax: 434.395.2821
trs: 711

September 25, 2013

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

Dear Ms. Mavredes:

We are providing this response in regard to your review of Information Security performed at Longwood University in conjunction with the audit of the June 30, 2013 financial statements.

Database Security

The University continues to work diligently in regards to database security. The following actions have been implemented to ensure that database security is improved:

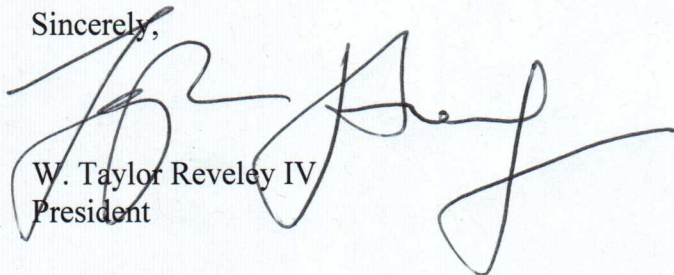
- ❖ Longwood University has developed an ITS standard for the usage and governance of super-user accounts that has been approved by the Chief Information Officer for Information Technology Services.
- ❖ Database user accounts have been configured to enforce strong passwords.
- ❖ The use of a centralized log server is currently in progress.



Office of the President

Should you have any questions or need additional information, please do not hesitate to contact me at (434) 395-2001.

Sincerely,



W. Taylor Reveley IV
President



September 25, 2013

Ms. Martha S. Mavredes, CPA
Auditor of Public Accounts
101 North 14th Street
Richmond, Virginia 23219

Thru: goran.gustavsson@apa.virginia.gov

Dear Ms. Mavredes:

Attached are the Virginia Lottery's responses to the *2013 State of Information Security in the Commonwealth of Virginia*.

#1: IT System Data Backup and Restoration

The Virginia State Lottery Department implemented substantial improvements to the physical security of backup media in transit in September, 2012.

#4: Risk Assessment

The Virginia State Lottery Department completed the remaining risk assessment in January, 2013.

#14: Firewall Security

The Virginia State Lottery Department completed the scheduled upgrade to the Firewall in September, 2012.

Sincerely,

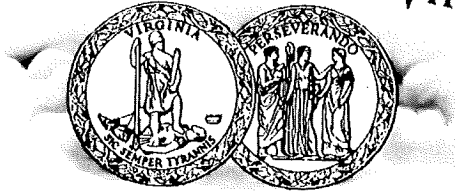
Paula I. Otto

MARK C. CHRISTIE
COMMISSIONER

JAMES C. DIMITRI
COMMISSIONER

JUDITH WILLIAMS JAGDMANN
COMMISSIONER

COMMONWEALTH OF VIRGINIA



JOEL H. PECK
CLERK OF THE COMMISSION
P.O. BOX 1197
RICHMOND, VIRGINIA 23218-1197

STATE CORPORATION COMMISSION

October 1, 2013

Ms. Martha S. Mavredes
Auditor of Public Accounts
PO Box 1295
Richmond, Virginia 23218

RE: 2013 State of Information Security in the Commonwealth of Virginia

Dear Ms. Mavredes:

Please include the following response to the 2013 State of Information Security in the Commonwealth of Virginia related to the finding on Database Security:

The State Corporation Commission (Commission) has made the recommended procedural and technical adjustments to the Database Administrator (DBA) activity logs as set out in the Fiscal Year 2012 audit report of the Commission. As a part of the corrective action plan for this finding, the Commission has developed a new policy on DBA privileged account usage and a new process to replicate the Oracle Audit logs to ensure that the integrity of the data is protected.

We appreciate the opportunity to provide a response to the report.

Sincerely,

A handwritten signature in black ink, appearing to read 'James C. Dimitri'.

James C. Dimitri
Commissioner

A handwritten signature in black ink, appearing to read 'Judith Williams Jagdmann'.

Judith Williams Jagdmann
Commissioner

A handwritten signature in black ink, appearing to read 'Mark C. Christie'.

Mark C. Christie
Commissioner



COMMONWEALTH of VIRGINIA

Department of the Treasury

MANJU S. GANERIWALA
TREASURER OF VIRGINIA

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

September 26, 2013

Ms. Martha Mavredes
Auditor of Public Accounts
PO Box 1295
Richmond, VA 23218

Dear Ms. Mavredes,

The Department of the Treasury (Treasury) appreciates the opportunity to respond to your 2013 State of Information Security in the Commonwealth of Virginia report. Treasury has placed the highest priority on resolving the information security audit management comment, Create Information Security Review Plan, recommended in February, 2013. Shortly thereafter, Treasury reviewed the agency's information systems and security plans. Subsequently, in July of 2013, Treasury finalized and submitted a three-year information security audit plan of information systems containing sensitive information, as required by the Commonwealth's information technology security audit standards.

Warm regards,

A handwritten signature in black ink, reading "Manju Ganeriwala".

Manju S. Ganeriwala



COMMONWEALTH of VIRGINIA

Cynthia C. Romero, MD, FAAFP
State Health Commissioner

Department of Health
P O BOX 2448
RICHMOND, VA 23218

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

October 3, 2013

Ms. Martha S. Mavredes, CPA
Auditor of Public Accounts
James Monroe Building
101 North 14th Street, 8th Floor
Richmond, VA 23219

Dear Ms. Mavredes:

The Virginia Department of Health (VDH) is providing this response to the findings of the 2013 State of Information Security in the Commonwealth of Virginia. VDH would like to comment specifically on the findings and progress made subsequent to the APA recommendations.

VDH currently manages database security and application development throughout the systems development life cycle. Recommendations made during the APA Audit, related to enhancements for the current procedures to better protect the system audit and transaction logs. VDH has implemented these recommendations to control access to these logs to protect their integrity while allowing our development staff to continue their work.

Following the APA recommendation on Business Impact Analysis (BIA) reporting, VDH immediately worked to update BIA documentation to include all business functions associated with each business unit within the agency. VDH focused resources, developed new Information Security Awareness Training, and incorporated the revised SEC501 requirements into BIA documents developed for agency business functions.

VDH believes that protecting the information to which we are entrusted is a cornerstone of our public health mission. The agency will continue to use opportunities such as this to enhance our information security as we provide critical services to the Commonwealth.

Sincerely,

A handwritten signature in blue ink, appearing to read "Debbie S. Condrey".

Debbie S. Condrey
Chief Information Officer