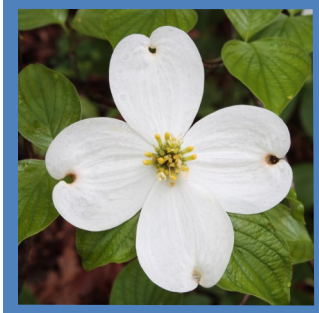



2015 STATE OF INFORMATION SECURITY IN THE COMMONWEALTH OF VIRGINIA

FOR THE PERIOD JULY 1, 2014 THROUGH JUNE 30, 2015

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

EXECUTIVE SUMMARY

The Auditor of Public Accounts (APA) performs information security reviews as part of its financial statement and performance audits of the Commonwealth's agencies and institutions of higher education. This report is a compilation of the information security findings issued as a part of these audits during fiscal year 2015. The APA reviews information security control areas by risk and not statistical sampling. Therefore, one cannot extrapolate the results in this report beyond the 50 agencies and institutions of higher education under audit in 2015.

The number of information security findings increased 86 percent in fiscal year 2015 compared to 2014. The most common cause of non-compliance with information security standards given by agencies is the lack of resources. More than half of the security findings occurred at ten of the agencies and institutions that we audited.

86% INCREASE IN SECURITY FINDINGS IN FISCAL YEAR 2015

A couple of factors may have partially contributed to this significant increase. The first factor is that the Commonwealth's Information Security Standard, SEC501, (CoVA Security Standard) has been updated to include more controls and to align with NIST, the federal government's information security standard, in the past two years. The second factor is that the APA increased information security audit hours from 6,000 to 6,600 in fiscal years 2014 and 2015, respectively. The increase in audit hours, in conjunction with better risk analysis tools, allows our office to better identify risky information security audit areas within individual organizations.

The most audited information security control category is access controls. In fiscal year 2015, access controls in more than half of the agencies we audited did not meet information security standards or best practices for managing or reviewing access controls to information technology systems that contain sensitive data.

For other information security control categories, including: audit and accountability, identification and authentication, system and communications protection, maintenance, planning, and personnel security, we tested the categories at agencies where we deemed it relevant to the audit objectives. The information security controls selected for testing at each agency are dependent on several risk factors and their applicability to the agency. At agencies where these control areas were tested, none of the agencies met the information security standards or best practices.

The number of agencies with multiple information security findings significantly increased since we last released a State of Information Security in the Commonwealth of Virginia report. In fiscal years 2012 and 2013, there were eight and ten agencies, respectively, that received multiple findings. In fiscal years 2014 and 2015, that number increased to 18 and 16 agencies, respectively, with multiple findings, an increase of 89 percent as compared to the preceding two fiscal years. A contributing factor to this increase may be the introduction of the NIST standard into the CoVA Security Standard and the addition of several more required information security controls.

Lastly, we reviewed database management systems and web applications at 17 and 15 agencies, respectively. We issued database management system findings to 11 agencies (65 percent) and web application findings to eight agencies (53 percent).

TABLE OF CONTENTS

INTRODUCTION

The Auditor of Public Accounts (APA) reviews information security controls as part of its financial statement and performance audits of executive and judicial branch agencies. Specifically, the APA reviews controls that belong to 19 main control areas, listed in the table on the right.

The *2015 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 (agencies) in the executive and judicial branches. The purpose of this report is to identify, on a statewide level, the weakest information security control areas and their trends and impact on securing citizens' data and uninterrupted access to on-line data.

Since our last report, *2013 State of Information Security in the Commonwealth of Virginia*, the Commonwealth's Information Security Standard, SEC 501 (CoVA Security Standard), adopted a significant portion of the National Institute of Standards and Technology's Special Publication 800-53 (NIST Security Standard). This adaptation, reflected in SEC501-07 effective November 19, 2012, allows the Commonwealth to easily align its information security controls with those required of federal government agencies.

While some agencies, such as Level II[1] and Level III[2] autonomous colleges and universities, are exempt from the CoVA Security Standard, the majority of the CoVA Security Standard controls are included in other national standards adopted by those entities, such as the International Organization for

INFORMATION SECURITY CONTROLS

- Access Control
- Audit & Accountability
- Awareness & Training
- Configuration Management
- Contingency Planning
- Identification & Authentication
- Incident Response
- Information Security Roles & Responsibilities
- IT Security Audits
- Maintenance
- Media Protection
- Personnel Security
- Physical & Environmental Protection
- Planning
- Risk Assessment
- Security Assessment & Authorization
- System & Communications Protection
- System & Information Integrity
- System & Services Acquisition

[1] Level II institutions with Information Technology autonomy from the Commonwealth: Christopher Newport University, George Mason University, James Madison University, Longwood University, Old Dominion University, Radford University, Mary Washington University, and Virginia Military Institute.

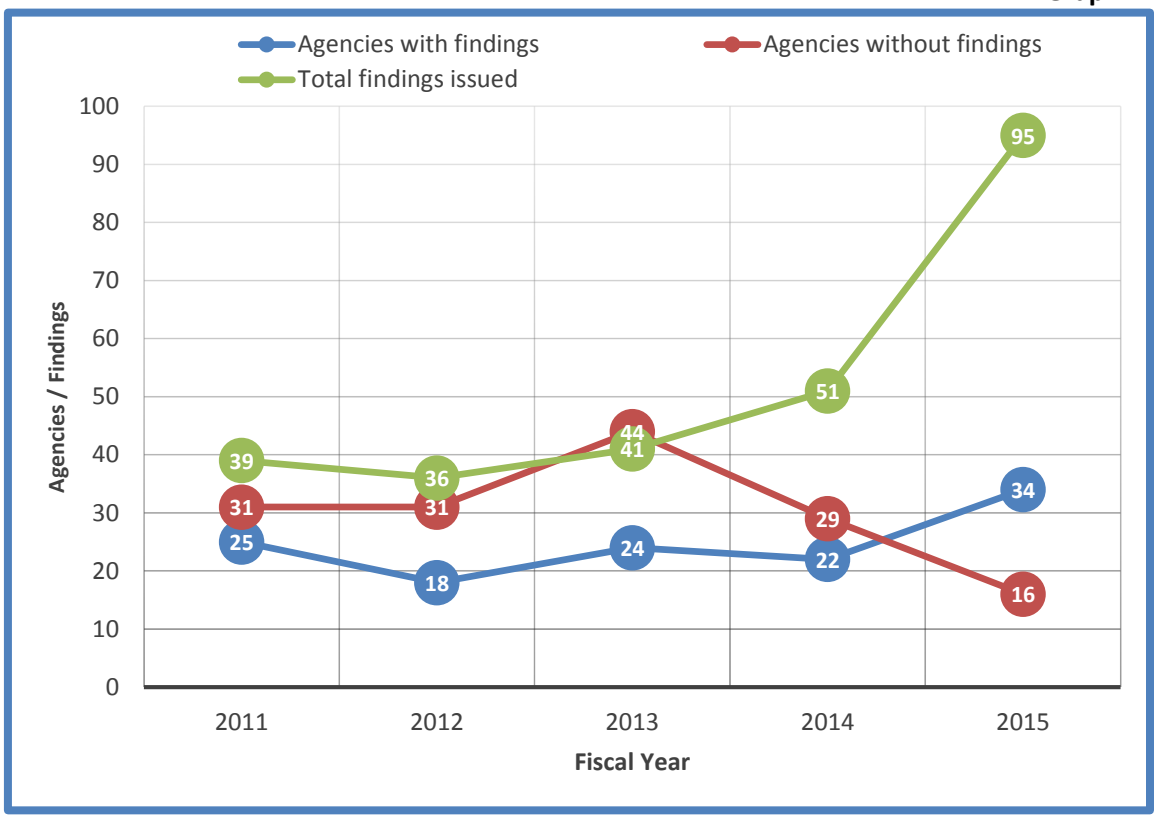
[2] Level III institutions with Information Technology autonomy from the Commonwealth: The College of William and Mary, University of Virginia, University of Virginia at Wise, Virginia Commonwealth University, and Virginia Polytechnic Institute and State University.

Standardization's security standard 27000 series (ISO 27000). Therefore, the APA makes the necessary control requirement adjustments while performing information security reviews for Level II and Level III autonomous colleges and universities.

Due to our risk evaluation process that determines which information security control areas to review, the statistics in this report are not derived from a sample and therefore cannot be extrapolated. However, if we simply look at the number of information security findings issued per fiscal year over the past five years, there is a significant increasing trend since fiscal year 2013. As shown in Graph 1, the increase in the number of findings has more than doubled in the past two years.

Information Security Findings by Fiscal Year

Graph 1



The increase in findings in 2013 and beyond coincides with the introduction of the NIST Security Standard controls into the CoVA Security Standard. The agency compliance date for the updated CoVA Security Standard, SEC501-07, was January 1, 2013. Since then, there have been three updates to the CoVA Security Standard, with the latest iteration being SEC501-09, and having an agency compliance date of August 1, 2015.

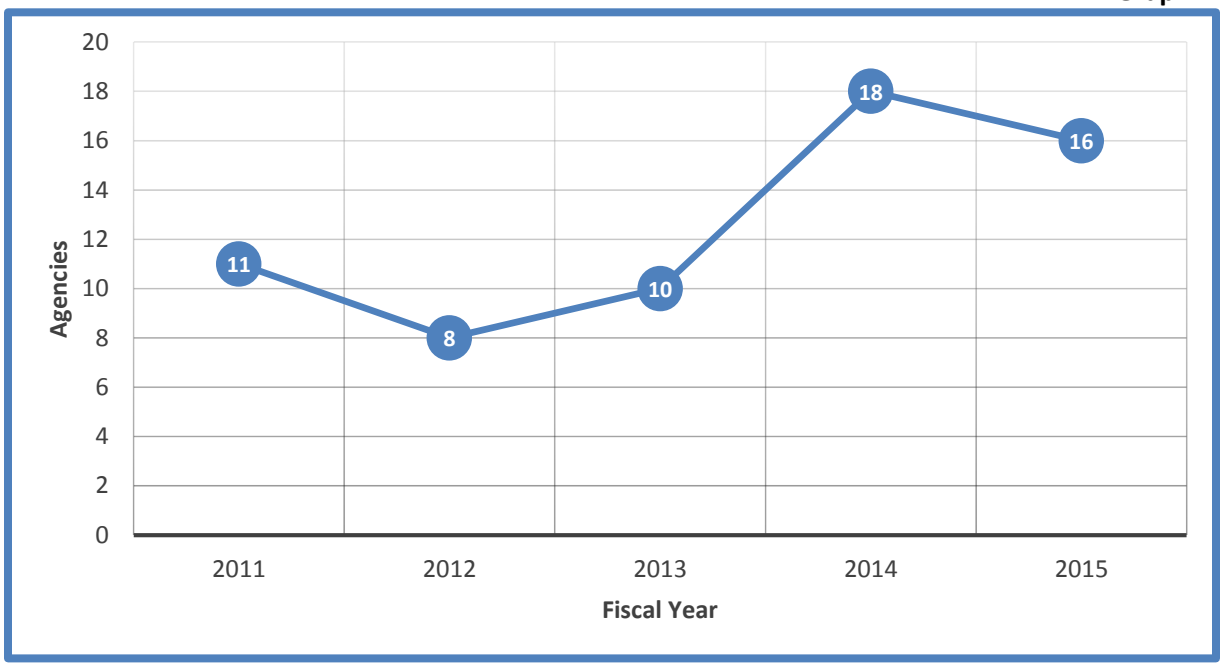
The number of findings increased 86 percent in fiscal year 2015 compared to 2014. Compared to fiscal year 2013, the number of findings in 2015 increased 132 percent. Most commonly, agencies cite a lack of resources as the main reason behind an information security control weakness in a finding. At other times, the reason may be attributed to poor organizational

or IT governance structure, responsibility discrepancies between the agency and the IT Infrastructure Partnership, or competing priorities.

Similarly, there is also an increasing trend of agencies receiving more than one information system security finding during an audit. As seen in Graph 2, the number of agencies with more than one finding has almost doubled in the most recent two fiscal years when compared to 2011, 2012, and 2013.

Agencies with More Than One Finding

Graph 2



In fiscal years 2012 and 2013, there were eight and ten agencies, respectively, that received multiple findings. In fiscal years 2014 and 2015, there were 18 and 16 agencies, respectively, with multiple findings. This reflects an 89 percent increase in agencies with multiple findings during fiscal years 2014 and 2015, compared to the preceding two fiscal years.

A couple of factors may have contributed to parts of these significant increases. The first factor is that the CoVA Security Standard has been updated to include more controls and to align with the NIST Security Standard, the federal government's information security standard, in the past two years. The second factor is that the APA increased information security audit hours from 6,000 to 6,600 hours in fiscal years 2014 and 2015, respectively. The increase in audit hours, in conjunction with better risk analysis tools, allows the APA to better identify risky information security audit areas within individual organizations.

The following sections in this report will focus on information security findings issued during fiscal year 2015. The analysis and categorization of these findings will give a picture of the weakest controls in the 50 agencies audited in the Commonwealth's information security posture.

METHODOLOGY AND SCOPE

The APA conducts its audits and issues financial statement and performance audit reports in accordance with generally accepted government auditing standards. This report is a compilation of the information security findings issued as a part of these audits during fiscal year 2015. To gain sufficient coverage over the general controls safeguarding the information audited, the APA also conducts information security reviews that use industry best practices and national and international information security standards as benchmarks.

During the course of an information security review, the agency's implemented information security controls are evaluated against that agency's approved information security policies, procedures, and processes. If the agency's policies, procedures, and processes do not consider certain parts of its adopted standard, we evaluate the implemented controls directly against the Commonwealth, national, or international standard adopted by the entity.

In addition to reviewing implementation of 19 main information security control areas, we use best practice benchmarks, such as those published by software vendors and organizations like the Center for Internet Security, to audit specific technologies, such as database management systems, server operating systems, and network infrastructure devices.

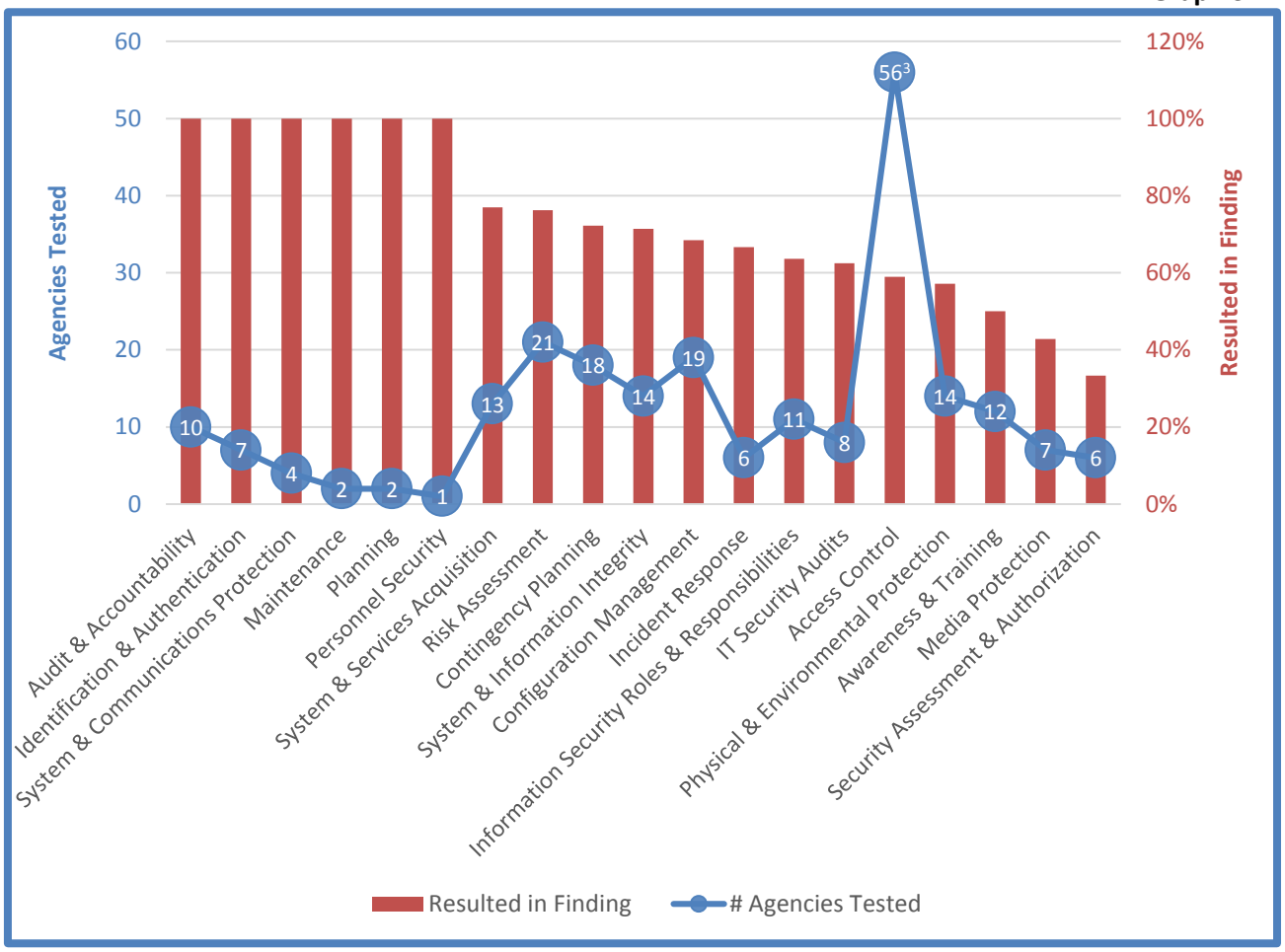
The scope of the information security controls we audit is determined by risk factors at the particular agency. It can range from reviewing one to reviewing all 19 main control areas. Certain controls are cycled and not reviewed during each audit period. The findings analyzed in this report were part of audit reports issued between July 1, 2014 and June 30, 2015.

FISCAL YEAR 2015 INFORMATION SECURITY FINDINGS ANALYSIS

In fiscal year 2015, we reviewed information security controls at 50 agencies. Our reviews resulted in no findings for 16 agencies (32 percent) and findings for 34 agencies (68 percent). Graph 3 illustrates the type of the issued findings categorized into the 19 major information security control areas. The detailed controls tested in each major control area are listed in Appendix A.

Fiscal Year 2015 Information Security Findings by Major Control Area

Graph 3



The bar graphs represent the percentage of reviews in a given control area that resulted in a finding. The control areas with the highest exception rate by percentage are sorted from left to right. The exception rate is calculated by dividing the number of findings with the total number of reviews

[3] Graph 3 Note: Access controls were reviewed at 48 agencies and eight community colleges that are part of the Virginia Community College System. Access controls was the only major information security control area reviewed at the community colleges during fiscal 2015. Therefore, the eight community colleges are not part of the total agency reviews in any of the other 18 control areas.

in a control area. For example, we reviewed the Audit & Accountability control area at ten agencies and all ten agencies received a finding, resulting in findings being issued to 100 percent of agencies tested in that control area.

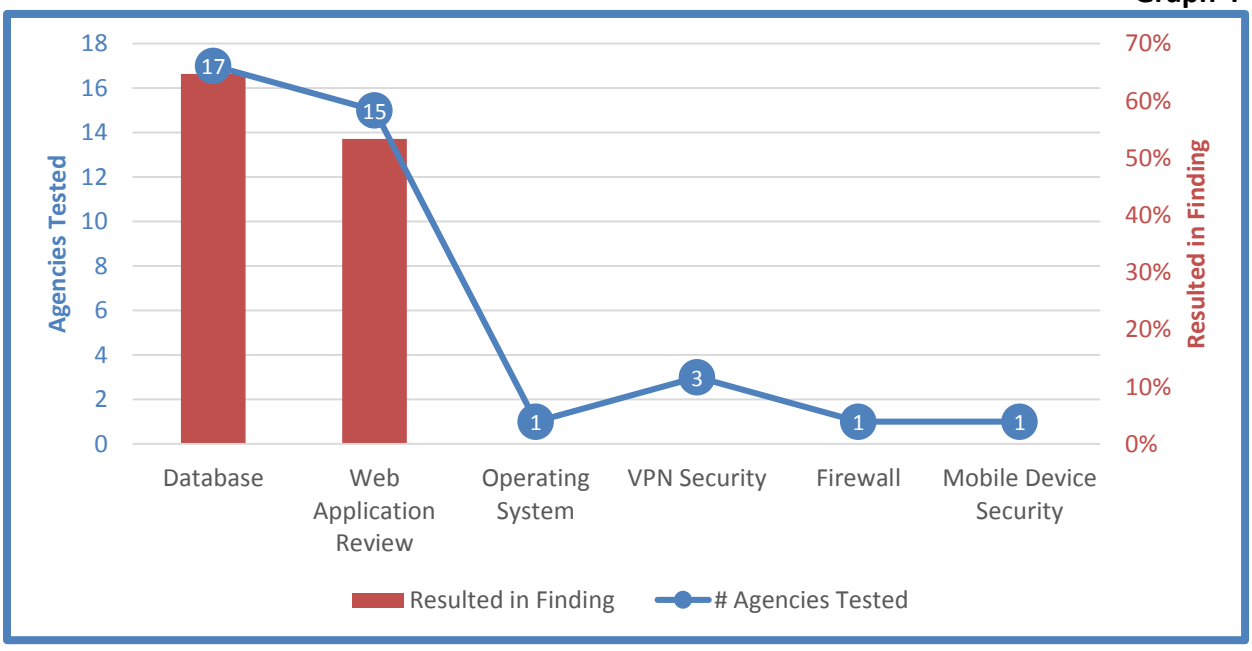
The line graph represents how many agencies the APA reviewed during fiscal year 2015 for a particular control area. Since our information security audit scope is established based on risk and not a sample, the exception rate cannot be extrapolated beyond the 50 agencies audited. The purpose for the line graph is to gauge weight to the exception rate in the bar graphs. For example, an exception rate of 100 percent across ten audited agencies carries more weight than an exception rate of 100 percent for one audited agency.

The APA also reviews major infrastructure applications, such as database management systems (Oracle and Microsoft SQL Server), server operating systems (UNIX and Windows), network infrastructure devices (firewalls, virtual private networks (VPN), routers), web applications, and mobile devices. We perform these audits by comparing agencies' implementations to the Commonwealth's and industry standards and best practices. As illustrated in Graph 4, we performed database reviews at 17 agencies, web application reviews at 15 agencies, an operating system review at one agency, VPN security reviews at three agencies, a firewall review at one agency, and a mobile device security review at one agency.

Due to the Commonwealth's IT Infrastructure Partnership, the APA does not perform audits of infrastructure devices (server operating systems, firewalls, VPNs, etc.) at executive branch agencies. These are audited by a firm that conducts an annual Service Organization Control audit of the infrastructure controlled by the IT Infrastructure Partnership. The APA does, however, perform reviews over these infrastructure devices at independent agencies, institutions of higher education, and the judicial system.

Fiscal Year 2015 Findings by Major Infrastructure Application

Graph 4



Sixty-five percent of the agency database audits conducted received findings relating to the way the agency sets up or manages their databases. The most common weakness is the lack of monitoring database user accounts with elevated privileges. These accounts are typically assigned to database administrators. Since these accounts can connect directly into the database, they do not adhere to the access rules established by the application that the database supports, such as PeopleSoft or Banner. For example, a database administrator user account can make changes directly to the data stored in the database without going through the access control and approval rules established in the business application it supports. Therefore, it is very important to log the activity of database administrator user accounts, protect these logs, and perform periodic reviews to identify an unauthorized change or disclosure.

Fifty-three percent of the agencies where we audited web applications security received findings relating to the way the agency develops and securely programs their web applications and configures the server operating system on which the web application rests. Since these web applications face the internet, securing the operating system on which the web application rests is important as it, too, connects directly to the internet. Additionally, using industry best practices when programming the web application is important to avoid unnecessary weaknesses that may result in a breach. The most common weaknesses in the web application findings relates to not properly securing operating system files, granting unnecessary privileges to operating system user accounts, and not having documented and approved policies, procedures, and baseline security configurations.

CONCLUSION

The Commonwealth's agencies continue to be challenged with keeping their information security programs in compliance with their applicable information security standard and technology-specific industry best practices. The most common cause for non-compliance cited by agencies is the lack of resources to keep up with changing and additional requirements introduced with each security standard update.

Access controls, including privileges assigned to employee user accounts with access to sensitive information systems, are a significant control that is reviewed at most agencies by the APA. While the requirements in this control area have been fairly consistent over the years, agencies continue to receive findings relating to ensuring that accounts adhere to the principle of least privilege and are periodically reviewed.

Lastly, the number of findings issued to agencies in fiscal year 2015 jumped to 95 from 51 in fiscal year 2014. Partially, this trend correlates to the additional requirements introduced in the CoVA Security Standard, starting in 2013, a lack of agencies' resources to implement those additional information security controls, and an improved risk analysis process used by the APA to establish information security audit scopes.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 1, 2015

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable John C. Watkins
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 **2015 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, 2014 through June 30, 2015, this report provides a state-wide perspective that highlights effective and ineffective information security controls throughout the Commonwealth.

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

Report Distribution

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

INFORMATION SECURITY CONTROL AREAS

The following is a list of the controls tested within each major control area. They are derived from the Commonwealth's Information Security Standard, SEC501. Our information security audits reviews these controls, where applicable, and make necessary adjustments to those entities that have adopted a different security standard, such as the ISO 27000 series.

Access Control (8.1-AC)

1. Access Control Policy and Procedures
2. Account Management
3. Account Management – Additional CoVA Requirements
4. Access Enforcement
5. Information Flow Enforcement
6. Separation of Duties
7. Least Privilege
8. Unsuccessful Logon Attempts
9. System Use Notification
10. System Use Notification – Additional CoVA Requirements
11. Session Lock
12. Session Termination
13. Permitted Actions Without Identification or Authentication
14. Remote Access
15. Remote Access – Additional CoVA Requirements
16. Wireless Access
17. Wireless Access – Additional CoVA Requirements
18. Access Control for Mobile Devices
19. Use of External Information Systems
20. Use of External Information Systems – Additional CoVA Requirements
21. Publicly Accessible Content

Awareness and Training (8.2-AT)

1. Security Awareness and Training Policy and Procedures
2. Security Awareness
3. Security Awareness – Additional CoVA Requirements
4. Role-Based Security Training
5. Security Training Records

Audit and Accountability (8.3-AU)

1. Audit and Accountability Policy and Procedures
2. Audit Event
3. Content of Audit Records
4. Audit Storage Capacity
5. Response to Audit Processing Failures
6. Audit Review, Analysis, and Reporting
7. Time Stamps
8. Protection of Audit Information
9. Audit Records Retention
10. Audit Generation
11. Monitoring for Information Disclosure

Security Assessment and Authorization (8.4-CA)

1. Security Assessment and Authorization Policies and Procedures
2. Information System Connections
3. Information System Connections – Additional CoVA Requirements
4. Security Authorization
5. Continuous Monitoring

Configuration Management (8.5-CM)

1. Configuration Management Policy and Procedures
2. Baseline Configuration
3. Baseline Configuration – Additional CoVA Requirements
4. Configuration Change Control
5. Configuration Change Control – Additional CoVA Requirements
6. Security Impact Analysis
7. Access Restrictions for Change
8. Configuration Settings
9. Least Functionality
10. Information System Component Inventory
11. Configuration Management Plan
12. Software Usage Restrictions
13. User-Installed Software

Contingency Planning (8.6-CP)

1. Contingency Planning Policy and Procedures
2. Contingency Planning Policy and Procedures – Additional CoVA Requirements
3. Contingency Plan
4. Contingency Training

5. Contingency Plan Testing and Exercises
6. Alternate Storage Site
7. Alternate Processing Site
8. Telecommunications Services
9. Information System Backup
10. Information System Backup – Additional CoVA Requirements
11. Information System Recovery and Reconstitution

Identification and Authentication (8.7-IA)

1. Identification and Authentication Policy and Procedures
2. Identification and Authentication (Organizational Users)
3. Identification and Authentication (Organizational Users) – Additional CoVA Requirements
4. Identifier Management
5. Authenticator Management
6. Authenticator Management – Additional CoVA Requirements
7. Authenticator Feedback
8. Cryptographic Module Authentication
9. Identification and Authentication (Non-Organizational Users)

Incident Response (8.8-IR)

1. Incident Response Policy and Procedures
2. Incident Response Policy and Procedures – Additional CoVA Requirements
3. Incident Response Training
4. Incident Response Testing and Exercises
5. Incident Handling
6. Incident Handling – Additional CoVA Requirements
7. Incident Monitoring
8. Incident Monitoring – Additional CoVA Requirements
9. Incident Reporting
10. Incident Reporting – Additional CoVA Requirements
11. Incident Response Assistance
12. Incident Response Plan

Maintenance (8.9-MA)

1. System Maintenance Policy and Procedures
2. Controlled Maintenance
3. Maintenance Personnel

Media Protection (8.10-MP)

1. Media Protection Policy and Procedures
2. Media Protection Policy and Procedures – Additional CoVA Requirements

3. Media Access
4. Media Storage
5. Media Storage – Additional CoVA Requirements
6. Media Transport
7. Media Sanitization
8. Media Sanitization – Additional CoVA Requirements
9. Media Use

Physical and Environmental Protection (8.11-PE)

1. Physical and Environmental Protection Policy and Procedures
2. Physical and Environmental Protection Policy and Procedures – Additional CoVA Requirements
3. Physical Access Authorizations
4. Physical Access Authorizations – Additional CoVA Requirements
5. Physical Access Control
6. Physical Access Control – Additional CoVA Requirements
7. Access Control for Output Devices
8. Monitoring Physical Access
9. Access Records
10. Power Equipment and Power Cabling
11. Emergency Shutoff
12. Emergency Power
13. Fire Protection
14. Temperature and Humidity Controls
15. Location of Information System Components

Planning (8.12-PL)

1. Security Planning Policy and Procedures
2. System Security Plan
3. System Security Plan – Additional CoVA Requirements
4. Rules of Behavior
5. Rules of Behavior – Additional CoVA Requirements

Personnel Security (8.13-PS)

1. Personnel Security Policy and Procedures
2. Personnel Screening
3. Personnel Termination
4. Personnel Transfer
5. Access Agreements
6. Third-Party Personnel Security
7. Personnel Sanctions

Risk Assessment (8.14-RA)

1. Risk Assessment Policy and Procedures
2. Security Categorization
3. Risk Assessment
4. Vulnerability Scanning
5. Vulnerability Scanning – Additional CoVA Requirements

System and Services Acquisition (8.15-SA)

1. System and Services Acquisition Policy and Procedures
2. Allocation of Resources
3. Life Cycle Support
4. Life Cycle Support – Additional CoVA Requirements
5. Information System Documentation
6. Information System Documentation – Additional CoVA Requirements
7. Security Engineering Principles
8. External Information System Services
9. Developer Configuration Management
10. Developer Security Testing
11. Development Process, Standards, and Tools
12. Developer-Provided Training
13. Developer Security Architecture and Design
14. Unsupported System Components

System and Communications Protection (8.16-SC)

1. System and Communications Protection Policy and Procedures
2. Application Partitioning
3. Security Function Isolation
4. Information in Shared Resources
5. Denial of Service Protection
6. Boundary of Protection
7. Transmission Integrity
8. Transmission Integrity – Additional CoVA Requirements
9. Cryptographic Key Establishment and Management
10. Use of Cryptography
11. Use of Cryptography – Additional CoVA Requirements
12. Public Key Infrastructure Certificates
13. Mobile Code
14. Voice of Internet Protocol
15. Secure Name / Address Resolution Service (Authoritative Source)
16. Session Authenticity

17. Protection of Information at Rest
18. Out-of-Band Channels
19. Port and I/O Device Access
20. Sensor Capability and Data
21. Sensor Capability and Data – Additional CoVA Requirements
22. Usage Restrictions

System and Information Integrity (8.17-SI)

1. System and Information Integrity Policy and Procedures
2. Flaw Remediation
3. Flaw Remediation – Additional CoVA Requirements
4. Malicious Code Protection
5. Malicious Code Protection – Additional CoVA Requirements
6. Information System Monitoring
7. Security Alerts, Advisories, and Directives
8. Spam Protection
9. Information Input Validation

Information Security Roles and Responsibilities (2)

1. Chief Information Security Officer (CISO)
2. Agency Head
3. Information Security Officer (ISO)
4. Privacy Officer
5. System Owner
6. Data Owner
7. System Administrator
8. Data Custodian
9. IT System Users

IT Security Audits (7)

1. IT Security Audits of IT Systems
2. Planning for IT Security Audits
3. IT Security Audit Scope
4. Documentation of IT Security Audits