



COMMONWEALTH of VIRGINIA

Virginia Information Technologies Agency

Samuel A. Nixon, Jr.
Chief Information Officer
Email: cio@vita.virginia.gov

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

TDD VOICE -TEL. NO.
711

March 7, 2011

The Honorable Robert F. McDonnell
Governor of Virginia
Patrick Henry Building, 3rd Floor
1111 East Broad Street
Richmond, Virginia 23219

The Honorable Charles J. Colgan
President pro tempore, Senate of Virginia
Post Office Box 396
Richmond, Virginia 23218

The Honorable William J. Howell
Speaker, Virginia House of Delegates
Post Office Box 406
Richmond, Virginia 23218

The Honorable James D. Duffey, Jr.
Secretary of Technology
Patrick Henry Building, 4th Floor
1111 East Broad Street
Richmond, Virginia 23219

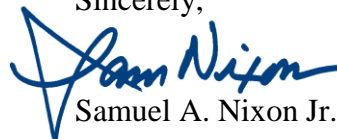
Dear Governor McDonnell, Mr. President pro tempore, Mr. Speaker, Mr. Secretary and members of the General Assembly:

The *Code of Virginia* §2.2-2009.C directs the Chief Information Officer (CIO) of the Commonwealth to prepare an Annual Report on Information Security in the Commonwealth relative to executive branch agencies, independent agencies and institutions of higher education.

I am pleased to report to you that, for this 2010 report, we conclude that significant, continued progress has been made in establishing and operating electronic information security programs adequate to safeguard the information of the Commonwealth; however, more work is needed, particularly in the area of sensitive system audits.

I welcome any assistance that the Governor and General Assembly can provide to ensure that the Annual Report on Information Security in the Commonwealth remains a valuable reference for Commonwealth information security decisions.

Sincerely,



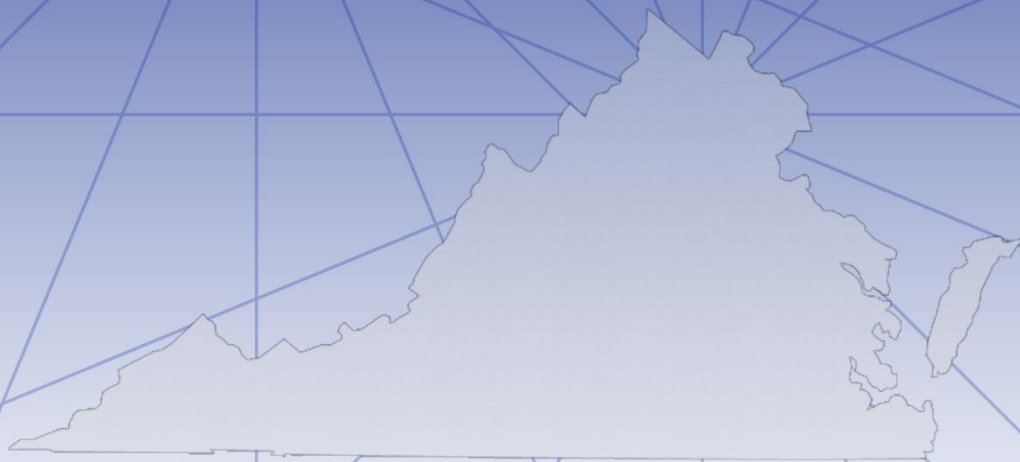
Samuel A. Nixon Jr.

c: The Honorable Martin Kent, Chief of Staff
Cabinet Secretaries
Walter J. Kucharski, Auditor of Public Accounts

Virginia Information Technologies Agency



2010 Commonwealth of Virginia Information Security Report



www.vita.virginia.gov

Prepared and Published by:
Virginia Information Technologies Agency

Comments on the
2010 Commonwealth of Virginia Information Security Report
are welcomed.

Suggestions may be conveyed electronically to
CommonwealthSecurity@VITA.Virginia.Gov

Please submit written correspondence to:

Samuel A. Nixon Jr.
Chief Information Officer of the Commonwealth
Virginia Information Technologies Agency
Commonwealth Enterprise Solutions Center
11751 Meadowville Lane
Chester, VA 23836
cio@vita.virginia.gov



Contents

Executive Summary	2
Background	3
Approach	3
2010 COV Information Security Program	4
Agency Information Security Efforts.....	7
Conclusion	8
Appendix - Detailed Information by Agency	10
Legend	10
Agency Information Security Datapoints	11



Executive Summary

This 2010 Commonwealth of Virginia (COV) Information Security Report is the third annual report to the Governor and the General Assembly and follows a baseline created in 2008 for assessing the strength of agency information security programs that have been established to protect Commonwealth information. The scope of this report is limited to the independent and executive branch agencies including higher education, and excluding charter and Tier II universities.

The detailed listing of agencies and specific security information points can be found in the Appendix.

The Commonwealth Information Security Program is comprised of work done cooperatively at the Commonwealth level and at each individual agency. The overall program is only as sound as the sum of these collective parts; therefore, the individual agency programs are of great importance.

For this 2010 report, we conclude that progress continues to be made by Commonwealth agencies in establishing and operating information security programs that are compliant with published policies and standards. In almost every case, the available metrics show positive trends and improvement. Executive branch consolidation and transformation efforts have demonstrated undeniable security benefits for agencies in the Commonwealth enterprise; however, those agencies that have not yet transformed continue to expend unnecessary resources and operate at an elevated level of risk to both themselves and the Commonwealth.

Although the metrics we have analyzed are overwhelmingly positive, there is one disconcerting area that deserves attention. Audit plan data suggests that agencies are not consistently auditing their sensitive systems at least once every three years as required by COV standards. These audits are a crucial part of the Commonwealth Information Security Program. Neglecting to perform these audits can undermine the entire Commonwealth program and place sensitive Commonwealth data at great risk.

The mission of having a strong Commonwealth Information Security Program is a journey without end as the threats and required defenses change daily; however, we believe that the Commonwealth is on the right path.

Background

The 2010 Commonwealth of Virginia Information Security Report is the third annual report to the Governor and the General Assembly as required by Section C of the Code of Virginia, §2.2-2009, *Additional Duties of the CIO relating to security of government information*. These duties include items such as:

- Directing the development of policies, procedures and standards for assessing security risks
- Determining the appropriate security measures and performing security audits of government electronic information
- Developing policies, procedures and standards that address the scope of security audits and the frequency of such security audits
- Receiving reports of security incidents while taking such actions as are necessary, convenient or desirable to ensure the security of the Commonwealth's electronic information and confidential data
- Making the annual report to the Governor and General Assembly regarding agencies' information security programs

To fulfill his information security duties under §2.2-2009, the CIO has established a Commonwealth Security and Risk Management (CSRM) directorate led by the Commonwealth CISO.

Approach

The 2010 COV Information Security Report follows a baseline created in 2008 for assessing the strength of the information security programs that have been established to protect Commonwealth information. The scope of this report is limited to the independent and executive branch agencies including higher education, but excludes charter and Tier II universities that have been exempted from compliance with Commonwealth policies and standards.

This report is not based on reviews of individual agency's information security programs, but rather is based on an analysis of data and information available to the Chief Information Security Officer (CISO) as of October 31, 2010. The COV Information Security Policy, Standard and Audit Standard require that certain data be reported by agencies to the CISO, and this data serves as the basis for the individual agency component of this report. This data includes whether an agency head has:

- Designated an Information Security Officer within the past two years
- Submitted a current Information Security Audit Plan for sensitive systems
- Provided Corrective Action Plans for completed information security audits
- Supplied Quarterly Status Updates for corrective actions
- Had personnel attend a voluntary Information Security Orientation session (Attendance is not required but indicates agencies that have taken extra action to learn how to build an effective agency information security program.)

The detailed listing of agencies and specific security data points can be found in the Appendix. We also utilized the reports from the Auditor of Public Accounts (APA), specifically the *2010 State of Information Security in the Commonwealth of Virginia* report. We analyzed security incidents reported by executive branch agencies. In addition, we utilized

information from the Commonwealth Information Technology Infrastructure Partnership relative to operational security changes associated with transformation activities.

2010 COV Information Security Program

Information Security Policies, Standards and Guidelines

The Commonwealth Information Security Program is composed of a policy and four standards to assist agencies in building and documenting an agency's information security program. The policy sets Commonwealth direction and establishes a framework that agency heads must follow in implementing information security programs. The four standards provide greater depth on the requirements of an agency information security program and address the topics of general information security, information security audits, removal of Commonwealth data from surplus computer hard drives and electronic media, and the use of non-Commonwealth devices for telework. If an agency has a way of conducting business that does not comply with the requirements, there is an exception process available.

Commonwealth Information Security Council

The Commonwealth Information Security Council consists of 12 Information Security Officers who have come together to strengthen the information security posture of the Commonwealth. The members come from all branches of government, including higher education and local government. They meet monthly as a council to provide direction for the Commonwealth's Information Security Program and have formed committees around the following four initiatives:

- Encryption
- Web applications
- Making information security an executive management priority
- Risk Management

The council's work includes such accomplishments as developing a Commonwealth of Virginia Identity and Access Management Trust Model, providing key information security messages for Information Security Awareness Month in October for inclusion in the Governor's Leadership Communiqué, giving input on data breach notification requirements and early adoption, and creating Commonwealth guidance for Web application security.

Commonwealth Information Security Officer's Advisory Group

The Commonwealth of Virginia's Information Security Advisory Group (ISOAG) is a very active group open to all state and local government personnel interested in improving the information security posture of the Commonwealth. The members share best practices and knowledge through regular monthly meetings and timely security alerts provided by Commonwealth Security. The group regularly interacts with national and state information security experts, and members are notified of upcoming cost-effective information security training opportunities.

In calendar year 2008, there were approximately 200 ISOAG members. Monthly meetings were held with an average attendance of 97 persons. In 2009, the membership grew to 389 persons, and monthly meeting attendance continued to average 97 persons. For 2010, the

membership grew to 481 persons, and monthly meeting attendance grew to an average 100 persons.

Information Security Orientation

Another Commonwealth program established to assist government personnel interested in learning about building and documenting an information security program in the Commonwealth is Information Security Orientation. This session provides participants with a background on why we care about security of information, what resources are available, and a walk through the actual steps in building and documenting an agency program utilizing the Commonwealth Information Security Policy, Standards and Guidelines. Commonwealth Security began the Information Security Orientation programs in March 2007 and has held 40 sessions with 381 people attending, including 98 from 49 Commonwealth independent and executive branch agencies, including higher education, within the last two years.

Commonwealth Information Security Incident Management

Section F of the Code of Virginia, *§2.2-603 Authority of agency directors* requires that executive branch agency directors report information technology security incidents to the CIO within 24 hours of discovery. The Commonwealth Security Incident Response Team classifies each of these security incidents into a category based on the type of activity. Reported security incidents are grouped into one of the following categories:

- Malware: Execution of malicious code such as viruses, spyware and key loggers
- Phishing: Theft or attempted theft of user information such as account credentials
- Physical Loss: Loss or theft of any COV resource that contains COV data
- Denial of Service: Loss of availability of a COV service due to malicious activity
- Unauthorized Access: Unauthorized access to COV data (This category also includes any security incident where it may be uncertain if a malicious party accessed COV data.)
- Inappropriate Use: Misuse of COV resources
- Other: Reports where the investigation determines the event is not a security incident

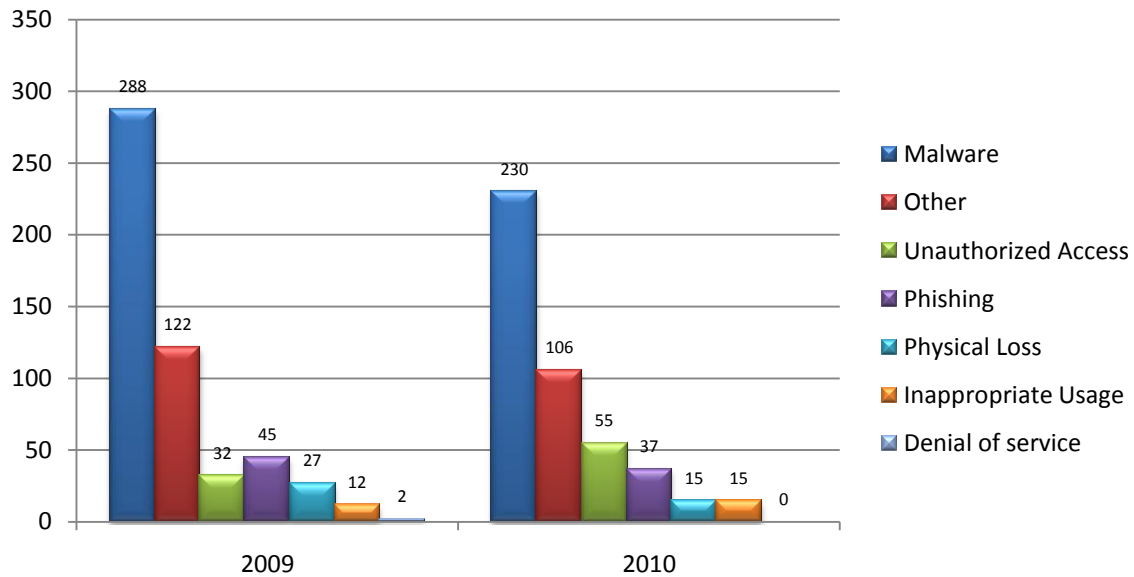


Figure 1: Security incidents by type per year

Through October 31, 2010, there were 458 information security incidents reported. Of those incidents, 230 were classified as using malicious software to modify or obtain Commonwealth information. The security incidents that involved unauthorized physical access to Commonwealth information primarily were due to lost or stolen equipment and accounted for 15 of the security incidents. Phishing attempts targeted at Commonwealth personnel accounted for 37 of the security incidents. Of the security incidents logged, 106 were classified as non-security incidents or unsuccessful attempts after a full investigation.

It is important to note that the Commonwealth's ability to protect, detect and react to these security threats has increased in proportion to the progress of the information technology infrastructure transformation. The result has been a significant decrease in security incidents throughout the partnership-supported agencies as security controls are implemented within the transformed environment.

Commonwealth Operational Security

From an operational security perspective, the largest initiative is found in the Commonwealth information technology infrastructure program with Northrop Grumman. Agencies either have undergone or will undergo transformation of their personal computers, servers, networks and messaging. The program security team provides numerous and redundant capabilities to robustly protect Commonwealth assets and data as part of the transformation process.

An improved security posture is one of the major benefits of the public-private partnership between the Commonwealth of Virginia and Northrop Grumman. The consolidated IT services model created by the partnership facilitates the enforcement of Commonwealth security standards, the collection of compliance metrics, the protection of electronic assets, and real-time response to cyber attacks. Documented security gaps arose through the practice of non-standard, individualized IT operations run independently by agencies. Many of these gaps now have been addressed by enterprise technologies provided by Northrop

Grumman and VITA together with operational policies provided by Commonwealth Security. As one of its duties, Commonwealth Security provides oversight of operational security activities in the transformed enterprise IT environment of executive branch agencies.

In April 2010, VITA conducted its annual disaster recovery test at the Southwest Enterprise Solutions Center (SWESC). The purpose of testing is to ensure readiness in the event of an actual disaster. Program staff members worked with disaster recovery customers to simulate a disaster and restore the hardware and software supporting critical services at SWESC. It is a comprehensive test and reveals the strengths and weaknesses in processes, procedures, documentation, staffing and hardware. Each year, we apply the lessons learned and set the bar higher in terms of the scope and complexity of testing in subsequent years. Overall, the testing process went very well and received positive feedback from customer agencies.

Agency Information Security Efforts

Positive metrics show that agencies have been working to build and document their information security programs. Our analysis of the specific data points reviewed indicates that progress has been made, but more work remains, particularly in the area of security audit.

Designation of an Information Security Officer within the past two years - A cornerstone in building an information security program is the agency head's designation of an Information Security Officer (ISO) every two years. The agency's ISO is responsible for maintaining a liaison with the CISO and developing and managing the agency's information security program.

Of the 82 agencies, 81 (99% - *up 1%*) agencies have designated an ISO within the past two years, and 1 (1%) has not.

Submission of a current information security audit plan for sensitive systems - Agency heads must take action to have each sensitive system audited at least once every three years and submit the plan for doing so to the CISO yearly. Placing reliance on any existing audit activity is encouraged. A security audit is an independent review to assess the effectiveness of the controls management implemented to safeguard the information processed by a system. This includes compliance with the Commonwealth Information Security Standard and any relevant federal or state laws or regulations.

Of the 82 agencies, 76 (93% - *up 4%*) have submitted a current information security audit plan, 2 (2%) have an expired audit plan, 2 (2%) have never submitted an audit plan, and 2 (2%) agencies have a current exception on file.

Provided corrective action plans for completed information security audits - For security audits that have been completed, corrective action plans are required to be submitted to the CISO quarterly identifying whether the agency head agrees or disagrees with the audit finding and, if in agreement, the actions planned to correct the vulnerabilities identified by the audit. If the agency head disagrees with the finding, a statement of the agency's position must be provided.

Of the 82 agencies, 36 (44% - *No change*) have submitted all corrective action plans, 6 (7%) have submitted some corrective action plans, 9 (11%) have not submitted any of the

corrective action plans due, and 27 (33%) have no corrective action plans due. For 2 (2%) agencies, this is not applicable as they have not yet submitted an audit plan, and 2 (2%) agencies have an exception on file.

Supplied quarterly updates for corrective action plans - For any completed security audits for which corrective action plans have been submitted, agencies are required to submit the status of outstanding corrective actions quarterly until the corrective action has been completed.

Of the 82 agencies, 22 (27% - up 5%) have submitted all updates, 4 (5%) agencies have submitted some updates, 1 (1%) agency has not submitted any updates, 41 (50%) agencies have no updates due. For 12 (15%) agencies, quarterly updates are not applicable since they have not submitted a security audit plan and/or a corrective action plan that was due, and 2 (2%) agencies have an exception on file.

Attendance at voluntary information security orientation session - Attendance at information security orientation is not required but indicates that agencies have taken extra action to learn how to build an effective agency information security program.

Of the 82 agencies, 49 (60% - down 9%) agencies have sent 98 persons to information security orientation, and 33 (40%) have not had a representative attend within the last two years.

Percentage of audit obligation completed (New for 2010) - As discussed above, agency heads must take action to have each sensitive system audited at least once every three years. The degree to which agency heads have fulfilled this audit obligation has been measured against the audit plans that each agency submitted beginning in 2007.

Of the 82 agencies, only 13 (16%) have completely fulfilled the obligation to have every sensitive system audited at least once every three years. At the other end of the spectrum, 8 (10%) agencies have not performed any audits or have not submitted evidence of an audit to the CISO. Finally, 33 (40%) agencies were not compliant with the requirement to submit an audit plan in 2007 and, therefore, cannot be measured.

**The detailed listing of agencies and specific security data points can be found in the Appendix .*

Conclusion

Building and strengthening Commonwealth of Virginia's information security is a shared effort. The foundation for the Commonwealth's Information Security Program is the collaborative effort of the Governor, General Assembly, Secretary of Technology and CIO. Building on that foundation is the work of agency heads, agency information security officers, agency technical support staff and every end user throughout the Commonwealth. Commonwealth Security continues to promote a number of information security awareness meetings and training sessions in an effort to educate and foster collaboration among information security professionals across the Commonwealth.

For this 2010 report, we conclude that progress continues to be made by Commonwealth agencies in establishing and operating information security programs that are compliant

with published policies and standards. In almost every case, the available metrics show positive trends and improvement. Executive branch consolidation and transformation efforts have demonstrated undeniable security benefits for agencies in the Commonwealth enterprise; however, those agencies that have not yet transformed continue to expend unnecessary resources and operate at an elevated level of risk to both themselves and the Commonwealth.

Although the metrics we have analyzed are overwhelmingly positive, there is one disconcerting area that deserves attention. Audit plan data suggests that agencies are not consistently auditing their sensitive systems at least once every three years as required by COV standards. These audits are a crucial part of the Commonwealth Information Security Program. Neglecting to perform these audits can undermine the entire Commonwealth program and place sensitive Commonwealth data at great risk.

Appendix - Detailed Information by Agency

Legend

APA 2010 Security Program Adequate (data from *2010 State of Information Security in the Commonwealth of Virginia*)

- Yes** - The agency has an adequate information security program that effectively mitigates risks
- No** - The agency does not have an adequate information security program that effectively mitigates risks

ISO Designated

- Yes** - The agency head has designated an Information Security Officer (ISO) for the agency within the past two years.
- No** - The agency head has NOT designated an ISO for the agency within the past two years.

Security Audit Plan Received

- Yes** - The agency head has submitted a current security audit plan for systems classified as sensitive.
- No** - The agency head has NOT had a security audit plan submitted for systems classified as sensitive.
- Exception** - The agency head has submitted, and the CISO has approved a temporary exception to allow time for developing the security audit plan.

Corrective Action Plans Received & Quarterly Updates Received

- Yes** - The agency head has submitted an adequate corrective action plan (CAP)/quarterly update (QU) for security audits.
- Some** - The agency head has submitted an adequate CAP/QU for some but NOT all security audits.
- No** - The agency head has NOT submitted an adequate CAP/QU for security audits.
- Not Due** - The agency head did not have security audits scheduled to be completed or has submitted a CAP within the last quarter and no QU is due.
- N/A** - Not applicable as the agency head has not submitted a security audit plan or a CAP that was due.

Attended IS Orientation (*not used in stoplight scoring)

The number indicates how many agency personnel have attended the optional Information Security Orientation sessions indicating they are taking additional, voluntary action to improve security at their agency akin to "Extra Credit!"

Percentage of Audit Obligation Completed (**not used in stoplight scoring this year)

- X%** - The percentage of audit work completed as measured against the agency's 2007 security audit plan
- N/C** - The agency did NOT submit a security audit plan in 2007, so the amount of audit work cannot be measured
- N/R** - The agency was not required to submit a security audit plan in 2007
- Exception** - In 2007, the agency head has submitted, and the CISO has approved a temporary exception to allow time for developing the security audit plan.

Agency Information Security Datapoints

Secretariat	Agency	APA 2010 Security Program Adequate	ISO Designated	Security Audit Plan Received	CAPs Received	Quarterly Updates Received	*IS Orientation Attended	**Percentage of Audit Obligation Completed
Administration	Compensation Board	Yes	Yes	Yes	No	N/A	1	0%
Administration	Dept. of General Services	Yes	Yes	Yes	No	N/A	3	0%
Administration	Dept. of Human Res. Mgmt	Yes	Yes	Yes	Yes	Not Due	1	100%
Administration	Dept. Min. Bus. Enterprise	No	Yes	Yes	Not Due	Not Due	0	N/C
Administration	Employee Dispute Resolution	Yes	Yes	Exception	Exception	Exception	1	0%
Administration	Human Rights Council	N/A	Yes	Yes	Not Due	Not Due	0	N/C
Administration	State Board of Elections	No	Yes	Expired	Some	No	0	50%
Ag. & Forestry	Dept. of Forestry	No	Yes	Yes	No	N/A	0	0%
Ag. & Forestry	Va. Dept. of Ag. & Cons. Serv.	Yes	Yes	Yes	Yes	Yes	1	66%
Commerce & Trade	Board of Accountancy	Yes	Yes	Yes	Yes	Not Due	0	100%
Commerce & Trade	Dept of Business Assistance	Yes	Yes	Yes	Yes	Not Due	0	N/C
Commerce & Trade	Dept. of Housing & Community Development	Yes	Yes	Yes	Some	Yes	0	29%
Commerce & Trade	Dept. of Labor & Industry	Yes	Yes	Yes	No	N/A	0	N/C
Commerce & Trade	Dept. of Mines, Minerals & Energy	Yes	Yes	Yes	Yes	Yes	0	83%
Commerce & Trade	Dept. of Professional & Occupational Regulation	Yes	Yes	Yes	Yes	Yes	1	100%
Commerce & Trade	Tobacco Indemnification Commission	N/A	Yes	Yes	No	N/A	1	N/C
Commerce & Trade	Va. Economic Development Partnership	Yes	Yes	Yes	Not Due	Not Due	1	N/C
Commerce & Trade	Va. Employment Commission	Yes	Yes	Yes	Some	Yes	0	Exception
Commerce & Trade	Va. National Defense Industrial Authority	Yes	Yes	Yes	Not Due	Not Due	0	N/C
Commerce & Trade	Va. Racing Commission	N/A	Yes	Yes	Yes	Not Due	1	N/C
Commerce & Trade	Va. Resources Authority	N/A	No	No	N/A	N/A	0	N/C
Education	Christopher Newport University	Yes	Yes	Yes	No	N/A	0	0%
Education	Dept. of Education	Yes	Yes	Yes	Yes	Not Due	1	100%
Education	Frontier Culture Museum of Va.	Yes	Yes	Yes	Not Due	Not Due	0	N/C
Education	Gunston Hall	Yes	Yes	Yes	Not Due	Not Due	1	N/C
Education	Jamestown - Yorktown Foundation	Yes	Yes	Yes	Yes	Yes	2	100%

Secretariat	Agency	APA 2010 Security Program Adequate	ISO Designated	Security Audit Plan Received	CAPs Received	Quarterly Updates Received	*IS Orientation Attended	**Percentage of Audit Obligation Completed
Education	Library of Va.	Yes	Yes	Yes	No	N/A	0	100%
Education	Norfolk State University	Yes	Yes	Expired	No	N/A	0	N/C
Education	Richard Bland College	Yes	Yes	Yes	Not Due	Not Due	0	100%
Education	Science Museum of Va.	Yes	Yes	Yes	Not Due	Not Due	1	N/C
Education	State Council of Higher Education for Va.	No	Yes	Yes	Not Due	Not Due	0	N/C
Education	University of Mary Washington	Yes	Yes	Yes	Yes	Yes	1	67%
Education	Va. Commission for the Arts	Yes	Yes	Yes	Not Due	Not Due	0	N/C
Education	Va. Museum of Fine Arts	Yes	Yes	Yes	Yes	Some	0	Exception
Education	Va. School for the Deaf and Blind	N/A	Yes	Yes	Not Due	Not Due	2	N/R
Education	Virginia State University	Yes	Yes	Yes	Yes	Yes	0	Exception
Finance	Dept. of Accounts	Yes	Yes	Yes	Yes	Not Due	1	N/C
Finance	Dept. of Planning & Budget	Yes	Yes	Yes	Yes	Not Due	0	N/C
Finance	Dept. of Taxation	Yes	Yes	Yes	Yes	Not Due	1	50%
Finance	Dept. of Treasury	Yes	Yes	Yes	Yes	N/A	1	7%
Health & Hum. Res.	Dept. of Health Professions	Yes	Yes	Yes	Not Due	Not Due	4	0%
Health & Hum. Res.	Dept. of Medical Assistance Services	Yes	Yes	Yes	Yes	Yes	2	100%
Health & Hum. Res.	Dept of Behavioral Health and Developmental Svcs	Yes	Yes	Yes	Yes	Yes	11	100%
Health & Hum. Res.	Dept. of Rehabilitative Services	No	Yes	Yes	Yes	Not Due	2	19%
Health & Hum. Res.	Dept. of Social Services	Yes	Yes	Yes	Not due	Not Due	4	11%
Health & Hum. Res.	Virginia Foundation for Healthy Youth TSF	N/A	Yes	Yes	Not due	Not Due	1	N/C
Health & Hum. Res.	Va. Dept. for the Aging	Yes	Yes	Yes	Yes	Not Due	1	Exception
Health & Hum. Res.	Va. Dept. of Health	Yes	Yes	Yes	Some	Some	2	20%
Natural Resources	Dept. of Conservation & Recreation	Yes	Yes	Yes	Yes	Yes	1	13%
Natural Resources	Dept. of Environmental Quality	Yes	Yes	Yes	Yes	Yes	2	100%
Natural Resources	Dept of Game & Inland Fisheries	Yes	Yes	Yes	Some	Some	3	N/C
Natural Resources	Dept. of Historic Resources	Yes	Yes	Yes	Not Due	Not Due	1	0%
Natural Resources	Marine Resources Commission	Yes	Yes	Yes	Yes	Yes	1	100%
Natural Resources	Va. Museum of Natural History	Yes	Yes	Yes	Not Due	Not Due	1	N/C
Public Safety	Alcoholic Beverage Control	Yes	Yes	Yes	Yes	Yes	5	100%

Secretariat	Agency	APA 2010 Security Program Adequate	ISO Designated	Security Audit Plan Received	CAPs Received	Quarterly Updates Received	*IS Orientation Attended	**Percentage of Audit Obligation Completed
Public Safety	Commonwealth's Attorney's Services Council	Yes	Yes	Yes	Not Due	Not Due	0	N/C
Public Safety	Dept. of Correctional Education	Yes	Yes	Yes	Yes	Yes	0	N/C
Public Safety	Dept. of Corrections	Yes	Yes	Yes	Yes	Yes	3	100%
Public Safety	Dept. of Criminal Justice Services	Yes	Yes	Yes	Yes	Yes	0	40%
Public Safety	Dept. of Fire Programs	Yes	Yes	Yes	Yes	Yes	0	N/C
Public Safety	Dept. of Forensic Science	Yes	Yes	Yes	Not Due	Not Due	0	N/C
Public Safety	Dept. of Juvenile Justice	Yes	Yes	Yes	Yes	Not Due	2	66%
Public Safety	Dept. of Military Affairs	No	Yes	No	N/A	N/A	0	N/C
Public Safety	Dept. of Veterans Services	Yes	Yes	Yes	Not Due	Not Due	1	N/C
Public Safety	Va. Dept. of Emergency Management	Yes	Yes	Yes	Not Due	Not Due	1	N/C
Public Safety	Va. State Police	Yes	Yes	Yes	Yes	Yes	1	87%
Technology	The Ctr for Innovative Tech.	Yes	Yes	Yes	Not Due	Not Due	0	N/C
Technology	Va. Info. Technologies Agency	Yes	Yes	Yes	Yes	Yes	3	70%
Transportation	Dept. of Motor Vehicles	Yes	Yes	Yes	Yes	Yes	1	N/C
Transportation	Dept. of Aviation	Yes	Yes	Yes	Not Due	Not Due	1	N/C
Transportation	Dept. of Rail & Public Trans.	Yes	Yes	Yes	Not Due	Not Due	0	0%
Transportation	Motor Vehicle Dealers Board	Yes	Yes	Yes	Not Due	Not Due	0	N/C
Transportation	Va. Dept. Of Transportation	Yes	Yes	Yes	Yes	Yes	6	66%
Independent	Indigent Defense Commission	Yes	Yes	Yes	Yes	Not Due	5	N/R
Independent	State Lottery Dept.	Yes	Yes	Yes	Not Due	Not Due	2	N/R
Independent	State Corporation Commission	Yes	Yes	Yes	No	N/A	3	N/R
Independent	Va. College Savings Plan	Yes	Yes	Yes	Yes	Not Due	1	N/R
Independent	Va. Office for Protection & Advocacy	No	Yes	Yes	Not Due	Not Due	1	N/R
Independent	Va. Retirement System	Yes	Yes	Yes	Some	Some	1	N/R
Independent	Va. Workers' Compensation Commission	Yes	Yes	Yes	Yes	Not Due	3	N/R
N/A	Office of the Governor	N/A	Yes	Exception	Exception	Exception	0	N/C
N/A	Office of the Attorney General	N/A	Yes	Yes	Not Due	Not Due	0	N/C