Virginia Information Technologies Agency

VITA

2011 Commonwealth of Virginia Information Security Report

www.vita.virginia.gov

Prepared and Published by:
Virginia Information Technologies Agency

Comments on the
2011 Commonwealth of Virginia Information Security Report
are welcome
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

Virginia Information Technologies Agency

Contents

Virginia Information Technologies Agency

2011 Information Security Report

Executive Summary

This 2011 Commonwealth of Virginia (COV) Information Security Report is the fourth annual report to the Governor and the General Assembly. It follows a baseline created in 2008 for assessing the strength of agency information technology (IT) security programs that have been established to protect Commonwealth data and systems. The scope of this report is limited to the independent and executive branch agencies, including higher education excluding charter and Tier II universities.

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

Limited progress has been made by agencies toward the establishment and operation of IT security programs that comply with published Commonwealth policies and standards. Commonwealth data will remain at risk until all agencies and VITA are able to allocate the resources needed to perform their information security obligations.

Despite increases in IT spend, agencies are not maintaining security programs to the degree needed to keep pace with an expanding use of IT. Data in this report indicate that many agencies are not fulfilling their IT security obligations. For example:

- Although the total number of audits of sensitive systems increased over the last three years, 57 percent of Commonwealth systems have not been audited.
- Of the 82 agencies, 20 (24 percent) have an expired IT security audit plan.

Shortcomings in agency IT audit practices in the face of increased spending indicate that investment in information security is not keeping pace with the growing use of IT.

Because the operational security program within VITA lacks the resources needed to maintain an effective security program, VITA must increase security staffing and funding to meet its statutory obligations. In order to respond to the 43 percent increase in IT security incidents that occurred in 2011, meet additional demands from enterprise-wide programs such as electronic data management and electronic health records, and oversee the increase in use of infrastructure services, VITA must increase security staffing and funding accordingly.

Due to the indicators of non-compliance with security requirements, Commonwealth Security and Risk Management (CSRM) will review how agency IT security programs are evaluated. The goal will be to identify where security programs are carrying the most risk. Once the risks are identified, limited resources that are available can be directed to mitigate the most significant risks. While this review may help mitigate the most egregious risks, the lack of resources may still impede progress. In addition, CSRM will begin to investigate the possibility of identifying what resources have been allocated historically to the information security programs at state agencies. This information will help establish where the gaps exist and if additional support from CSRM or another state entity would be appropriate.

In today's digital world of information sharing and online services, the Commonwealth of Virginia must remain vigilant in its mission to maintain a strong IT security program. As new technologies emerge and threats evolve, it is imperative that the Commonwealth meet the challenge of ensuring that the data with which it is entrusted continue to be protected.

Background

The 2011 Commonwealth of Virginia Information Security Report is the fourth 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 electronic government 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 Chief Information Officer of the Commonwealth (CIO) has established a Commonwealth Security and Risk Management (CSRM) directorate led by the Commonwealth Chief Information Security Officer (CISO).

Approach

The 2011 COV Information Security Report builds on 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 excluding charter and Tier II universities that have been exempted from compliance with Commonwealth policies and standards.

This report is not based on field reviews of individual agencies' information security programs, but rather on an analysis of data and information reported to the CISO as of Dec. 31, 2011. 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, including whether an agency head has:

- Designated an information security officer (ISO) within the past two years
- Submitted a current IT security audit plan for sensitive systems
- Provided corrective action plans for completed information security audits
- Supplied quarterly status updates for corrective actions
- Audited sensitive systems within the required three-year period
- Had personnel attend a voluntary information security orientation session (Attendance is not required, but it indicates whether agencies 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. Historically, reports from the Auditor of Public Accounts (APA), specifically the *State of Information Security in the Commonwealth of Virginia*, have been utilized; however, this year the report was unavailable. In addition, CSRM analyzed security incidents reported by executive branch agencies and utilized information from the Commonwealth information technology infrastructure.

2011 COV Information Security Program

Information Security Policies, Standards and Guidelines

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

Commonwealth Information Security Council

The Commonwealth Information Security Council consists of 12 ISOs who come together to strengthen the IT 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 three initiatives:

- Risk management
- Cloud-based services
- Health care IT

The council's work includes providing input to revisions of standards, providing messages for Information Security Awareness Month in October for inclusion in the Governor's Leadership Communiqué and creating Commonwealth guidance for Web application security.

Commonwealth Information Security Officer's Advisory Group

The Commonwealth of Virginia's Information Security Officers Advisory Group (ISOAG) is a dynamic group open to all state and local government personnel. Its focus is on using IT security knowledge exchange to improve the security posture of the Commonwealth. The members share best practices and knowledge through monthly meetings and timely security alerts provided by CSRM. The group interacts with national and state experts and receives updates to the Commonwealth information security program. Members are notified of training opportunities. In 2011, ISOAG monthly meeting keynote speakers included representatives from the Federal Bureau of Investigation (FBI), Blue Coat, Good Technologies, RSA, Verizon, Zscaler and SANS.

ISOAG membership has grown from approximately 200 members in its inaugural year (2008) to 524 members at the end of 2011. Quality keynote speakers and a desire within the Commonwealth IT security community to maintain current knowledge and understanding of threats and trends have contributed to strong attendance, with an average of 105 attendees per meeting. These meetings have been made available through webinars, helping security professionals save travel time and costs. In addition, information security professionals have the opportunity to earn continuing professional education credits (CPEs), a requirement necessary for security professionals to maintain their security certifications and memberships in global security organizations. There is no cost to the attendee.

Information Security Orientation

The information security orientation program is an opportunity for agency personnel with IT security roles and responsibilities to gain a better understanding of the Commonwealth's security framework. Orientation includes a discussion of IT security in the Commonwealth, standard best practices, available resources, compliance, and a walk-through of how to build and document an agency program. The content is adjusted to include trending information and improvements in the framework, and offers a platform for discussion and feedback. Since 2007, 44 sessions have been held and attended by 425 state agency representatives of independent, judicial and executive branch agencies, including institutions of higher education. The orientation program contributes to a strong Commonwealth IT security program. Eighty individuals from 45 agencies attended orientation in 2011.

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 IT security incidents to the CIO within 24 hours of discovery. The Commonwealth Security Incident Response Team (CSIRT) classifies each of these security incidents into a category based on the type of activity.

The data collected in 2011 shows that the Commonwealth continues to be a target for malicious attacks. This year reflected a significant increase – 43 percent – in the number of security incidents. While the increase was primarily due to malware infections in the environment, the high number of incidents shows the challenge that the Commonwealth faces in keeping data secure.

Reported security incidents are grouped into one of the following categories:

- Malware - Execution of malicious code such as viruses, spyware and keyloggers
- 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 usage - Misuse of COV resources
- Other - Reports where the investigation determines the event is not a security incident

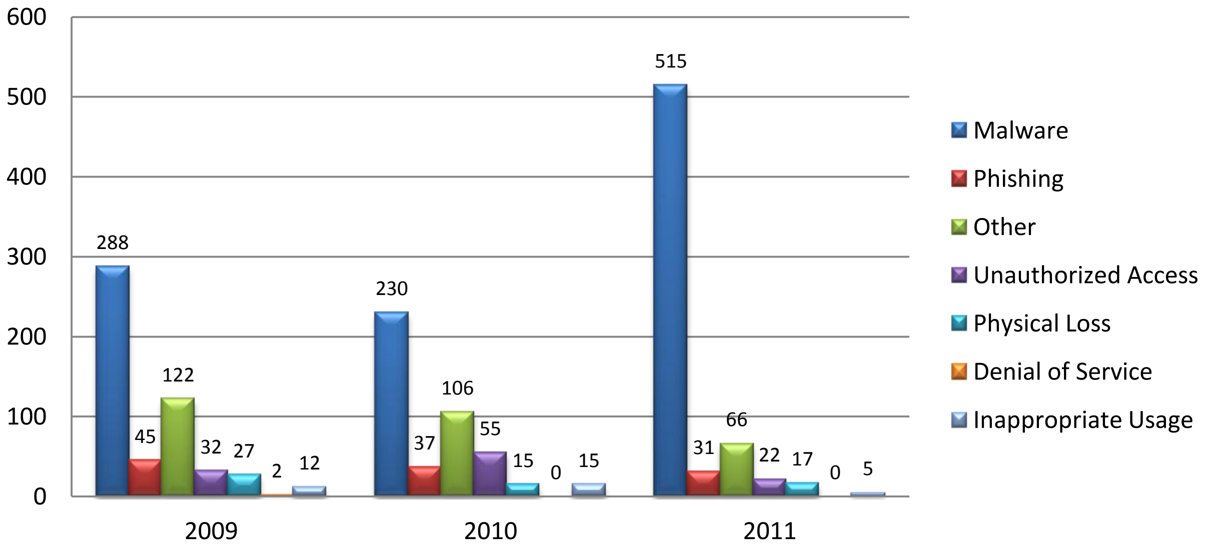


Figure 1: Security incidents by type per year

There are additional indicators of the size of the cyber threat to Virginia shown in the data collected from Virginia's primary data center. The Commonwealth received 118,486,625 alerts, or approximately four attacks per second, of malicious activity. While the vast majority of attacks were not successful, the number of attack attempts continually challenges Commonwealth IT security personnel to adapt quickly and defend against the constantly shifting cyber threat to prevent data compromise.

Email is a tool heavily utilized throughout the Commonwealth to carry out daily business. Security tools must be in place because of the heavy usage. Last year, the Commonwealth filtered 705,996,847 spam messages and blocked 33,575 viruses from reaching Commonwealth assets. Security personnel constantly are fine-tuning the security environment to prevent unsolicited and malicious email from reaching the state employees' computers. As a result, users do not realize how much spam is blocked from their mailboxes.

One of the additional services that the security incident response program provides is the gathering of cyber intelligence information affecting the Commonwealth. While a formal intelligence program is not funded, CSRM provides cyber intelligence information for both agencies and law enforcement within the Commonwealth. CSRM continues to develop relationships with state, federal and local partners. Some of the more notable relationships involve the Multi-State Information Analysis and Sharing Center (MS-ISAC), the FBI, United States Computer Emergency Response Team (US-CERT) and the Department of Homeland Security (DHS). Information about security issues regularly is exchanged with these entities and the state information security community. As a result of these relationships, the CSIRT has worked with more than 50 state agencies, 23 localities, 13 colleges and universities, and five public school systems to provide notifications of website defacements, compromised accounts and malware infections.

The information received from Commonwealth partners includes data involving both Commonwealth government and its citizens. A majority of the data affecting citizens is reported by MS-ISAC as keylogger events. A keylogger event is recorded when CSRM is notified that malicious software designed to record data transactions between the victim and a website or online service belonging to Commonwealth government has been used. CSRM works with state agencies to identify the victims of keylogging in order to alert them that their data has been compromised by a malicious third party. In 2011, the Commonwealth experienced 24,962 keylogger events. As a result of these events, personally identifiable information (PII) of 2,105 citizens was exposed.

Commonwealth Operational Security

While agencies that are part of the IT infrastructure program with Northrop Grumman have a significantly improved security posture as a result of security controls put into place by the program, the lack of staff and funding to oversee the program is beginning to impact the overall security posture of the program. As IT spend increases, it is critical that staffing and funding be increased to accommodate that change.

VITA has only one security operations staff member managing the entire IT infrastructure program with Northrop Grumman. To evaluate and manage the implementation of the program, additional resources are needed. These resources are critical to provide oversight and timely responses to security requirements of agency projects and programs. In addition, current staffing is not sufficient to ensure that the program remains in compliance with the security standards, regulations and policies that apply to the program. The Commonwealth is subject to a number of federal and industry regulations that, if not adhered to, can result in significant penalties or the inability of agencies to operate their programs. The lack of staffing puts the oversight of the IT infrastructure program security posture at risk, ultimately resulting in significant risk to Commonwealth data.

In addition to the staffing deficit in the IT infrastructure program with Northrop Grumman, there is not enough staffing to support the security needs of the rest of the Commonwealth. Between 2010 and 2011, there was a 43 percent increase in the number of security incidents throughout the Commonwealth. That increase is equivalent to approximately two additional security incidents per calendar day for an entire year. CSRM currently has only one security incident engineer to support all incidents within the Commonwealth. With the significant increase in cyber attacks against the Commonwealth, additional staff is necessary to investigate the risk of these incidents to the Commonwealth.

In addition, there is only one security architect for the Commonwealth. The enterprise security architect is responsible for ensuring that proper security controls exist for agency IT architecture and programs. The architect assists agencies with security programs to make sure they meet the necessary security standards and regulations. Additionally, the architect staffs enterprise-wide initiatives, such as the electronic health records program and the electronic data management program, to ensure proper security controls are in place. The demand for the security architect's services has increased significantly over the past few years. In order to meet the needs of the Commonwealth and ensure that proper security controls are in place, additional staff and resources should be applied. The operational security program within VITA does not have enough staff and resources to support the needs of the Commonwealth and therefore is unable to fully implement the assigned legislative requirements. In order to provide proper operational support the security staffing and funding at VITA must adjust in order to address and manage the threat that the Commonwealth faces and the number of IT projects the Commonwealth implements. If these adjustments are not made the integrity of the operational security program is at risk.

Agency Information Security Program

The Commonwealth IT Security and IT Security Audit Standards require that agencies develop and maintain an agency IT security program. Agencies are required to appoint an ISO and identify their sensitive systems, develop an IT security audit plan and conduct IT security audits on those systems at a minimum of every three years.

Agencies continued to make progress in completing audits of their sensitive systems, but a significant number of agencies did not complete audits as required. Several agencies failed to submit documentation necessary to maintain their overall IT security program. However, the primary cause for the downward trend in overall ratings is attributed to agencies not completing their audits within the designated three-year period.

Designation of an information security officer within the past two years - A cornerstone of building an IT security program is the agency head's designation of an ISO every two years. The agency's ISO is responsible for maintaining a relationship with the CISO and developing and managing the agency's program.

Of the 82 agencies, 80 agencies (98 percent) have designated an ISO within the past two years.

⬇ **Down 1 percent**

from 2010

Submission of a current information security audit plan for sensitive systems - A security audit is an independent review to assess the effectiveness of the controls implemented to safeguard the information stored and/or processed by a system. The Commonwealth uses security audits to determine if the proper controls exist to adequately protect Commonwealth data. The controls of each system are evaluated by the requirements in the Commonwealth Information Security Standard, federal laws, state laws and regulations. Agency heads must take action to have each sensitive systems audited every three years and submit a corrective action plan status to the CISO yearly.

Of the 82 agencies, 62 (76 percent) have submitted a current information security audit plan and 20 (24 percent) have an expired audit plan.

⬇ **Down 17 percent**

from 2010

Provided corrective action plans for completed information security audits - Corrective action plans are required to be submitted to the CISO quarterly in order to show the results of the agency security audits. These results include information indicating whether the agency head agrees or disagrees with the audit finding and, if in agreement, the actions planned to correct the vulnerabilities identified in the audit. If the agency head disagrees with the finding, a statement of the agency's position must be provided.

Of the 82 agencies, 63 (76 percent) have submitted all corrective action plans, or not had corrective action plans due; one (1 percent) has submitted some of its corrective action plan; and 18 (22 percent) have not submitted any of the corrective action plans due.

⇔ **No Change**

from 2010

Supplied 2011 quarterly updates for corrective action plans - In order to track the progress of remediation for submitted corrective action plans, agencies are required to provide quarterly updates to the CISO. These updates contain the status of outstanding corrective actions and the expected completion date. The updates continue until the corrective actions have been completed.

Of the 82 agencies, 66 (80 percent) have submitted all updates or did not have updates due; nine agencies (11 percent) have submitted some of the updates; and seven agencies (nine percent) have not submitted any updates.

⬆ **Up 4 percent**

from 2010

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

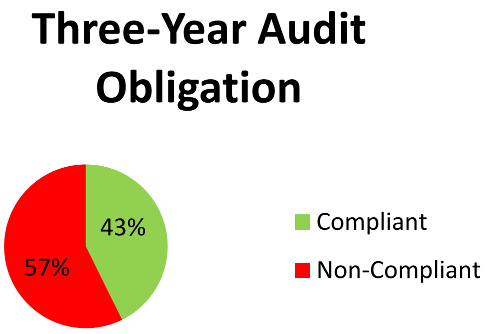
Of the 82 agencies, 45 agencies (55 percent) have sent a total of 80 persons to information security orientation, and 37 (45 percent) have not had a representative attend within the last two years.

⬇ **Down 4 percent**

from 2010

Percentage of audit obligation completed - As discussed previously, 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 using the audit plans each agency submitted beginning in 2007.

Of the 82 agencies, 35 (43 percent) have completely fulfilled the obligation to have every sensitive system audited at least once every three years, and 19 (23 percent) have partially completed their audit obligation. At the other end of the spectrum, 28 agencies (34 percent) have not performed any audits or have not submitted evidence of an audit for their systems in the last three years to the CISO.



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

Conclusion

Limited progress continues to be made by Commonwealth agencies in establishing and operating information security programs that comply with published policies and standards. Moreover, the small number of agencies that have not yet transformed continue to expend unnecessary resources and operate at an elevated level of risk to both the agency and the Commonwealth.

The information provided herein suggests that agencies are not applying sufficient resources to maintain their IT security programs. While agencies audited a larger number of sensitive systems this year, the data shows that agencies are not consistently auditing their sensitive systems at least once every three years as required. These audits are an integral part of the Commonwealth information security program as they verify that necessary security controls are in place to protect Commonwealth data. Neglecting to perform the audits prevents an accurate assessment of the Commonwealth IT security program and places sensitive Commonwealth data at risk.

In addition to the lack of agency resources to complete the necessary audits, a significant number of agencies failed to submit required documentation such as updated IT security audit plans. The combination of agencies not meeting their requirements and the inability to provide documentation indicating they are maintaining security programs resulted in a downward trend of agency ranking in 2011.

To determine the root cause of agencies being unable to comply with security requirements, CSRM will be reviewing how agency IT security programs are evaluated. The review will identify where agencies are experiencing the most significant risk. Once the risks are identified, the limited resources that are available can be directed to mitigate the most significant risks. While this review may help mitigate the risks as effectively as possible, lack of resources may still impede progress. In addition, CSRM will investigate the possibility of identifying what resources have been allocated historically to state agency IT security programs. Identifying this information will help establish where gaps exist and if additional support from CSRM or another state entity would be appropriate.

In conjunction with the review of agency resources, CSRM will evaluate the operational security needs at VITA. CSRM will use the review to make a recommendation about adjustments needed to the staff and resources in order to manage effectively the Commonwealth operational security program.

Building and strengthening the Commonwealth of Virginia’s IT security is a shared effort. The foundation for security programs requires executive leadership and has had the support of the Governor, General Assembly, Secretary of Technology and CIO of the Commonwealth. With the support of this leadership, CSRM has built a strong program. To maintain the integrity of this program, CSRM has begun making changes to help identify where the Commonwealth may have weaknesses. In addition, CSRM will continue to investigate the lack of resources to maintain agency programs. The goal is to prevent further decline in agency programs.

Furthering the information security program and building on the existing foundation is the work of agency heads, agency information security officers, agency technical staff and every end user throughout the state government. The continued success of the program will require the participation of all agencies and agency leadership. Though this report has identified potential issues, information security within the Commonwealth remains a top priority.

Appendix - Detailed Information by Agency

Legend

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 submitted a security audit plan for systems classified as sensitive.

Expired - Audit plan on file is does not cover the required 3 year period.

Corrective Action Plans Received & Quarterly Updates Received

X% - The percentage of due corrective action plans & quarterly updated received based on the security audit plan

N/A - Not applicable as the agency did not have corrective action plans or quarterly updated due or the agency head has not submitted a security audit plan.

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

X% **-** The percentage of audit work completed as measured against the agency's security audit plans over the past three years.

Agency Information Security Datapoints

Secretariat	Agency Acronym	Agency Name	ISO Designated	Security Audit Plan Received	Percent CAPS Received 2011	Total Percentage QU 2011	IS Orientation Attended	Percentage Of Audit Obligation Complete
Administration	CB	Compensation Board	Yes	Yes	0	N/A	0	0
Administration	DMBE	Dept. Min. Bus. Enterprise	Yes	Expired	N/A	N/A	1	0
Administration	DGS	Dept. of General Services	Yes	Yes	N/A	N/A	0	0
Administration	DHRM	Dept. of Human Res. Mgmt	Yes	Yes	0	N/A	0	100
Administration	EDR	Employee Dispute Resolution	Yes	Yes	100	100	1	100
Administration	HRC	Human Rights Council	Yes	Yes	N/A	N/A	1	100
Administration	SBE	State Board of Elections	Yes	Expired	N/A	0	1	50
Agriculture & Forestry	DOF	Dept. of Forestry	Yes	Yes	100	N/A	1	100
Agriculture & Forestry	VDACS	Va. Dept. of Ag. And Cons. Serv.	Yes	Yes	100	100	1	100
Commerce & Trade	BOA	Board of Accountancy	Yes	Yes	N/A	N/A	1	0
Commerce & Trade	DBA	Dept. of Business Assistance	Yes	Expired	N/A	N/A	0	0
Commerce & Trade	DHCD	Dept. of Housing and Community Development	Yes	Yes	100	100	0	80
Commerce & Trade	DOLI	Dept. of Labor & Industry	Yes	Expired	0	N/A	0	0
Commerce & Trade	DMME	Dept. of Mines, Minerals & Energy	Yes	Yes	100	25	5	57
Commerce & Trade	DPOR	Dept. of Professional & Occupational Regulation	Yes	Yes	N/A	25	1	100

Secretariat	Agency Acronym	Agency Name	ISO Designated	Security Audit Plan Received	Percent CAPS Received 2011	Total Percentage QU 2011	IS Orientation Attended	Percentage Of Audit Obligation Complete
Commerce & Trade	TIC	Tobacco Indemnification Commission	Yes	Expired	0	N/A	0	0
Commerce & Trade	VEDP	Va. Economic Development Partnership	Yes	Yes	N/A	N/A	0	0
Commerce & Trade	VEC	Va. Employment Commission	Yes	Yes	100	100	0	22
Commerce & Trade	VRC	Va. Racing Commission	Yes	Yes	100	N/A	1	100
Commerce & Trade	VRA	Va. Resources Authority	No	Expired	N/A	N/A	0	0
Education	CNU	Christopher Newport University	Yes	Yes	0	N/A	1	0
Education	DOE	Dept. of Education	Yes	Yes	100	100	1	78
Education	FCMV	Frontier Culture Museum of Va.	Yes	Expired	N/A	N/A	0	100
Education	GH	Gunston Hall	Yes	Expired	N/A	N/A	1	0
Education	JYF	Jamestown - Yorktown Foundation	Yes	Yes	N/A	100	0	100
Education	LVA	Library of Va.	Yes	Expired	0	N/A	0	0
Education	NSU	Norfolk State University	Yes	Expired	N/A	N/A	4	0
Education	RBC	Richard Bland College	Yes	Yes	100	N/A	1	100
Education	SMV	Science Museum of Va.	Yes	Yes	N/A	N/A	0	100
Education	SVHEC	Southern Virginia Higher Education Center	Yes	Yes	N/A	N/A	0	100
Education	SCHEV	State Council of Higher Education for Va.	Yes	Expired	0	N/A	0	0
Education	UMW	University of Mary Washington	Yes	Yes	100	33.33	1	100
Education	VCA	Va. Commission for the Arts	Yes	Yes	N/A	N/A	0	100
Education	VMFA	Va. Museum of Fine Arts	Yes	Yes	N/A	0	2	50

Secretariat	Agency Acronym	Agency Name	ISO Designated	Security Audit Plan Received	Percent CAPS Received 2011	Total Percentage QU 2011	IS Orientation Attended	Percentage Of Audit Obligation Complete
Education	VSDB	Va. School for the Deaf and Blind	Yes	Yes	0	N/A	0	0
Education	VSU	Virginia State University	Yes	Expired	100	36.36	0	78
Executive	OAG	Office of the Attorney General	Yes	Yes	N/A	N/A	2	100
Executive	GOV	Office of the Governor	Yes	Yes	N/A	N/A	0	100
Finance	DOA	Dept. of Accounts	Yes	Yes	N/A	100	1	25
Finance	DPB	Dept. of Planning & Budget	Yes	Expired	N/A	0	0	100
Finance	TAX	Dept. of Taxation	Yes	Yes	100	100	0	90
Finance	TD	Dept. of Treasury	Yes	Yes	0	N/A	0	0
H & HR	DBHDS	Dept of Behavioral Health and Developmental Svcs	Yes	Yes	N/A	0	1	100
H & HR	DHP	Dept. of Health Professions	Yes	Yes	0	N/A	2	0
H & HR	DMAS	Dept. of Medical Assistance Services	Yes	Yes	N/A	N/A	2	0
H & HR	DRS	Dept. of Rehabilitative Services	Yes	Yes	60	48.15	2	45
H & HR	DSS	Dept. of Social Services	Yes	Yes	0	50	5	22
H & HR	VDH	Va. Dept. of Health	Yes	Yes	N/A	76.19	0	22
H & HR	VFHY	Virginia Foundation for Healthy Youth TSF	Yes	Yes	N/A	0	0	100
Independent	IDC	Indigent Defense Commission	Yes	Yes	N/A	100	4	100
Independent	SCC	State Corporation Commission	Yes	Yes	100	100	2	75

Secretariat	Agency Acronym	Agency Name	ISO Designated	Security Audit Plan Received	Percent CAPS Received 2011	Total Percentage QU 2011	IS Orientation Attended	Percentage Of Audit Obligation Complete
Independent	SLD	State Lottery Dept.	Yes	Yes	100	0	2	100
Independent	VCSP	Va. College Savings Plan	Yes	Yes	N/A	N/A	1	100
Independent	VOPA	Va. Office for Protection & Advocacy	Yes	Yes	0	N/A	1	0
Independent	VRS	Va. Retirement System	Yes	Yes	100	75	0	72
Independent	VWC	Va. Workers' Compensation Commission	Yes	Yes	N/A	N/A	1	17
Natural Resources	DGIF	Dept of Game & Inland Fisheries	Yes	Yes	0	N/A	3	0
Natural Resources	DCR	Dept. of Conservation & Recreation	Yes	Yes	100	75	0	67
Natural Resources	DEQ	Dept. of Environmental Quality	Yes	Yes	N/A	N/A	2	100
Natural Resources	DHR	Dept. of Historic Resources	Yes	Yes	100	N/A	0	100
Natural Resources	MRC	Marine Resources Commission	Yes	Yes	100	100	1	100
Natural Resources	VMNH	Va. Museum of Natural History	Yes	Expired	0	N/A	0	0
Public Safety	ABC	Alcoholic Beverage Control	Yes	Yes	100	100	3	100
Public Safety	CASC	Commonwealth's Attorney's Services Council	Yes	Expired	N/A	N/A	0	100
Public Safety	DCE	Dept. of Correctional Education	Yes	Yes	100	100	2	100
Public Safety	DOC	Dept. of Corrections	Yes	Yes	100	100	4	100
Public Safety	DCJS	Dept. of Criminal Justice Services	Yes	Expired	0	N/A	1	0

Secretariat	Agency Acronym	Agency Name	ISO Designated	Security Audit Plan Received	Percent CAPS Received 2011	Total Percentage QU 2011	IS Orientation Attended	Percentage Of Audit Obligation Complete
Public Safety	DFP	Dept. of Fire Programs	Yes	Yes	N/A	100	0	100
Public Safety	DFS	Dept. of Forensic Science	Yes	Yes	100	N/A	0	50
Public Safety	DJJ	Dept. of Juvenile Justice	Yes	Yes	N/A	100	2	67
Public Safety	DMA	Dept. of Military Affairs	Yes	Expired	N/A	N/A	0	0
Public Safety	DVS	Dept. of Veterans Services	Yes	Yes	100	N/A	1	100
Public Safety	DEM	Va. Dept. of Emergency Management	Yes	Yes	N/A	N/A	2	0
Public Safety	VSP	Va. State Police	Yes	Yes	100	100	0	100
Technology	ITA	The Ctr for Innovative Tech.	Yes	Expired	0	N/A	2	0
Technology	VITA	Va. Info. Technologies Agency	Yes	Yes	100	100	1	50
Transportation	DOAV	Dept. of Aviation	Yes	Yes	0	N/A	2	0
Transportation	DMV	Dept. of Motor Vehicles	Yes	Yes	0	0	1	100
Transportation	DRPT	Dept. of Rail & Public Trans.	Yes	Expired	N/A	N/A	0	0
Transportation	MVDB	Motor Vehicle Dealers Board	Yes	Yes	N/A	N/A	0	100
Transportation	VDOT	Va. Dept. Of Transportation	Yes	Yes	100	100	2	100
Transportation	VPA	Virginia Port Authority	No	Expired	N/A	N/A	0	0