



COMMONWEALTH of VIRGINIA

Virginia Information Technologies Agency

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

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

TDD VOICE -TEL. NO.
711

May 29, 2013

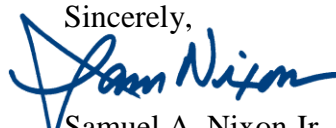
The Honorable Robert F. McDonnell
Governor of Virginia
Patrick Henry Building, 3rd Floor
1111 East Broad Street
Richmond, Virginia 23219

General Assembly of Virginia
c/o Division of Legislative Automated Systems
910 Capitol Street, General Assembly Building, 6th Floor
Richmond, Virginia 23219
Attn: Laura Wilborn

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

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

I welcome any input regarding the enclosed *Annual Report on Information Security in the Commonwealth* to ensure that it continues to be a valuable reference for the Commonwealth's IT security decisions.

Sincerely,

Samuel A. Nixon Jr.

c: The Honorable Martin Kent, Chief of Staff
The Honorable James D. Duffey, Jr., Secretary of Technology
Cabinet Secretaries

Virginia Information Technologies Agency



*2012 Annual Report
on Information Security (IT)
in the Commonwealth*



www.vita.virginia.gov

Prepared and Published by:
Virginia Information Technologies Agency

Comments on the
2012 Annual Report on Information Security (IT) in the Commonwealth 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



Contents

Executive Summary	2
2012 COV Information Security Program.....	3
Information Security Policies, Standards and Guidelines	3
Commonwealth Operational Security	4
Commonwealth Information Security Council	5
Commonwealth Information Security Officer’s Advisory Group	5
Information Security Orientation.....	6
Commonwealth IT Risk Management Program	6
Business Impact Analysis (BIA)	7
Risk Assessment.....	7
Risk Assessment Findings	7
Threat Metrics	7
Commonwealth Cyber Threat and Attack Analysis	7
Agency Information Security Program	12
Methodology.....	16
Appendix I - Agency Information Security Datapoints - Dashboard.....	18
Appendix II - 2012 Overall Audit Program Scores	22
Appendix III - 2012 Complete Risk Profile IT Security Audit Findings.....	26



2012 Information Security Report

Executive Summary

This 2012 Annual Report on Information Security (IT) in the Commonwealth is the fifth annual report by the Chief Information Officer of the Commonwealth (CIO) to the Governor and the General Assembly. As directed by §2.2-2009 (C) of the Code of Virginia, the CIO is required to identify those agencies that have not implemented acceptable policies, procedures and standards to control unauthorized uses, intrusions or other security threats. In accordance with §2.2-2009 (C), the scope of this report is limited to independent and executive branch agencies, including Tier I institutions of higher education. This report does not address Tier II and Tier III institutions that have been statutorily exempted from compliance with Commonwealth policies and standards.

To fulfill his information security duties under §2.2-2009, the CIO has established a Commonwealth Security and Risk Management (CSRM) directorate within the Virginia Information Technologies Agency (VITA). CSRM is led by the Commonwealth's Chief Information Security Officer (CISO). This report has been prepared by CSRM on behalf of the CIO, and it follows a baseline created by CSRM in 2008 to assess the strength of agency information technology (IT) security programs that have been established to protect Commonwealth data and systems. A detailed listing of agencies and their specific security information concerns can be found in the appendix.

The last year has not seen any noticeable improvement in agency IT security programs. Currently, 58 percent of agencies have not implemented acceptable policies, standards and procedures to control unauthorized uses, intrusions and other security threats. The failure of implementation results in unknown levels of risk in the Commonwealth IT environment. Additionally, the three agencies that have not yet transformed to the new IT infrastructure continue to operate at an elevated level of risk to both the agency and the Commonwealth and expend unnecessary resources. Since agencies are not applying the proper resources to meet the current IT security audit and information security program requirements, CSRM will investigate introducing a standard to enforce information security and information security audit programs.

Agencies are not submitting documentation indicating whether compensating controls have been implemented for open findings or what amount of residual risk is identified. As a result, these agencies are unable to identify how much risks they are subject to. The audit and risk documentation processes are two important ways that agency IT risks are identified to agency management. Agencies can use this information when making decisions concerning prioritization and allocation of resources. CSRM is investigating methods to identify and report the amount of agency risk.

CSRM reviewed the evaluation of IT security programs and identified areas for improvement. The existing evaluation relies primarily on submission of documentation that show whether the agency complied with specified requirements. CSRM is moving to a risk-based evaluation of the information security program. Over the next year, CSRM will introduce methods to identify the most significant IT risks that affect the Commonwealth and methods to prioritize the remediation of those risks.

Security is not being adequately included in the lifecycle planning of IT systems.

End-of-life planning for IT systems and applications is not sufficiently addressing the need to upgrade hardware and software that is no longer supported by a vendor. Continued use of unsupported hardware and software is costly and puts Commonwealth information at a high risk level. In addition to the risks posed by vulnerabilities in unsupported systems, the talent pool for antiquated systems and applications diminishes over time, leading to even higher costs to maintain the system. CSRM will investigate implementing processes to require that agencies provide plans to update or replace out of support or soon to be out-of-support IT systems.

Survey results, as well as the status of the information security programs as a whole, indicate that agency ISOs and information security programs do not have adequate resources.

Agency security personnel and management are not receiving enough security training and education to understand the information security risk carried by the agency. Unless agencies understand the impact of the risk carried, decisions could be made that potentially result in adverse consequences. CSRM is investigating how to account for resource allocation as part of agency remediation plans.

Lack of improvement in the security posture of the Commonwealth IT environment can lead to numerous undesirable outcomes. Approximately 10 percent of reported business functions and their corresponding systems impact the safety of Commonwealth citizens and employees. An information security event impacting a system supporting these business functions could result in adverse impact on the security of data, safety of those depending on the business function and Commonwealth finances. A significant data breach, such as the 2012 data breaches in South Carolina and Utah, results in significant costs. It is estimated that the South Carolina Department of Revenue data breach will cost that state more than \$20 million and the Utah Department of Health data breach is estimated to cost between \$2 million and \$10 million. Unless the Commonwealth improves its overall IT security posture, Virginia could experience a similar breach.

Information Security Program

The primary objectives for the Commonwealth's cyber security strategy are:

- Prevent cyber attacks against the Commonwealth's critical infrastructures
- Prevent theft of Commonwealth data
- Reduce the Commonwealth's vulnerability to cyber attacks
- Increase the Commonwealth's ability to respond quickly and effectively against cyber attacks, minimizing damage and recovery time
- Establish cyber security knowledgeable workforce
- Establish cyber security resources at Commonwealth agencies
- Improve cyber security situational awareness
- Identify and remediate risks to Commonwealth data
- Establish IT infrastructure impact analysis

Information Security Policies, Standards and Guidelines

The Commonwealth IT security program is composed of a policy and four standards designed to assist agencies in building and documenting their security program. The policy sets the Commonwealth's direction and establishes a framework that agency heads must follow in implementing IT security programs. The four standards provide a greater depth of information 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. An exception process is available if an agency must conduct business that does not comply with the requirements.

In 2012, CSRM focused on efficiency by streamlining the information security program. The Commonwealth created a new information security standard, SEC 501-07, which is based on the federal information security requirements published by the National Institutes of Science and Technology (NIST SP800-53 revision 3). The new standard retains the same numbering convention to maintain alignment and streamline future revisions. In addition to leveraging the information security research conducted by the National Institute of Standards and Technology, the alignment with federal standards will limit the need for Commonwealth agencies to comply with two different security frameworks. CSRM is working to create template policies for agencies to use and will continue to update the Commonwealth's policies, standards and guidelines as threats evolve.

Commonwealth Operational Security

The addition of new CSRM staff over the last year helped to reduce the effects of staffing shortages on the information security program. A security architect was added to CSRM and an operations analyst was recruited and will be added in early 2013. The addition of these positions improves CSRM's ability to address existing oversight and architecture requirements. However, due to the increase in regulatory requirements, enterprise applications and agency requests, CSRM still lacks sufficient staff to address agency requests to complete security reviews.

Additional staff is needed in CSRM to respond to the continuing increase in security incidents. Over the last year, the number of security incidents increased by 20 percent; this increase came on top of the 40 percent increase in security incidents in the previous year. Security incident trending has been increasing over time to the point of having more than two incidents every day. Unless the Commonwealth commits additional staff to security, the state will remain at risk of theft of data and/or compromise of the IT infrastructure.

In 2012, CSRM focused on reviewing the Commonwealth's operational environment and identifying areas for improvement. The first part of the year, CSRM focused on addressing the significant resource shortage affecting CSRM. While VITA was able to add some resources there are still significant gaps, some of which were exacerbated by the addition of secretariat-wide IT projects that require dedicated CSRM resources to address privacy and data security issues identified in implementation. If this trend continues, additional security staff will be required to meet the timelines proposed for these projects.

To improve the Commonwealth's security posture the second half of 2012, CSRM focused on overhauling VITA's security infrastructure and obtaining Commonwealth risk information. The security infrastructure overhaul included adding a filter that reduced malicious web traffic, updating antivirus and intrusion detection technology, upgrading event correlation engine, and adding real-time network inspection devices. The combination of these changes has resulted in a significant decrease in the number of attacks affecting Commonwealth systems and added insight into the situational awareness of the VITA environment. The results also impacted the number of security incidents recorded. While the numbers decreased in the short term, malicious third parties already have begun to adjust their methods of intrusion with some levels of success. VITA will continue to monitor and adjust defenses accordingly; however, the incident trend is expected to begin increasing again throughout 2013.

One of the operational challenges identified in 2012 involves the use of outdated software in the environment. Agencies are having difficulty ensuring proper maintenance of software

lifecycle plans. Whether the product is created by an agency or purchased from a third party, agencies appear to be unable to meet the requirement that their applications (and application dependencies) are maintained in a way that ensures the ability to receive security updates and patches. The inability to remain current with security updates and patches puts the agency IT environment at risk of compromise and/or data loss. Agencies will either need to identify ways to streamline their software lifecycle process for testing or implement additional security controls that will increase operating costs.

While CSRM expects that the risk management program will help identify some of the most significant risks, CSRM will investigate implementing a corresponding risk remediation process. The intent of the process will be to both notify the appropriate parties of the agency risk and offer a possible solution with a corresponding implementation time frame. The risk remediation process will help agencies by enabling VITA to assign resources for remediation when the agency is unable to do address issues in a timely fashion. VITA's intent is to assist agencies with addressing risks in the event agencies do not have the resources to address the risks.

Commonwealth Information Security Council

The Commonwealth Information Security (IS) Council consists of 12 information security officers (ISO) who come together to work to strengthen the IT security posture of the Commonwealth. The members come from all branches of government, including higher education and local government. The IS Council's work includes providing input to revisions of standards and providing messages for the Information Security Awareness Month in October for inclusion in the Governor's Leadership Communiqué. The IS Council meets monthly to provide direction for the Commonwealth's information security program and formed committees to address the following three initiatives for 2012:

- Risk management
- Cloud-based services
- Healthcare IT

In 2012, the Risk Management Committee focused on how to increase awareness of the importance of risk management through education, support and analysis. The Cloud-Based Services Committee released a white paper, *Cloud Computing: Security Considerations and Recommendations for Agencies*, while the Healthcare IT Committee has been involved in the strategic healthcare IT initiatives within the Commonwealth and the Risk Management committee.

As a result of increased participation in the information security community, the IS Council has had increased participation in the advisory groups around the following new initiatives:

- Information Security Officer Manual
- Information Security Conference
- Bring Your Own Device Security Strategy

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. The focus is IT security knowledge exchange to improve the 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 2012, ISOAG monthly meeting keynote speakers included representatives from the following: Cisco Systems, Dominion Power, McAfee, Virginia Commonwealth

University, 83rd Network Operations Squadron, Information System Security Association, University of Virginia, Federal Bureau of Investigation, RSA, Transportation Security Administration and Syrinx Technologies.

ISOAG membership has grown from approximately 200 members in its inaugural year (2008) to 565 members at the end of 2012. 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 of 1,377 attendees, an average of 115 attendees per meeting, in 2012. These meetings have been made available through webinars, which help security professionals save travel time and cost. In addition, information security professionals have the opportunity to earn continuing professional education credits, a requirement necessary for security professionals to maintain their security certifications and memberships in global security organizations. There is no cost to the attendees.

CSRM is investigating the possibility of recording the ISOAG meetings and making digital archives available online.

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. Forty-eight sessions since 2007 have been attended by 469 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. Forty-four individuals from 27 agencies attended orientation in 2012. Agencies only need to send someone once every two years.

Commonwealth IT Risk Management Program

In 2012, the Commonwealth IT Risk Management Program was created. The purpose of this program is to:

- Identify where the most significant risks to the Commonwealth exist
- Prioritize resources and efforts based on risk
- Ensure the agency leadership understands risks
- Set a risk threshold for the Commonwealth as a whole

Agencies were required in 2012 to submit their existing risk assessments, business impact analyses, and threat metrics to CSRM. While the number of submissions was low, this is the first year of the program and CSRM will continue to assist agencies with completing these necessary steps to be able to make better risk-based security decisions.

To identify the risks within the Commonwealth, CSRM will use the data provided and compare agencies to identify critical business functions and the supporting IT systems. The systems identified as critical will be reviewed to ensure that they are prioritized appropriately and given necessary resources and effort. In the coming year CSRM will work toward creating reports from the collected information that will allow agency heads to understand risks. CSRM plans to utilize the results of the risk analysis in order to set a risk threshold for the Commonwealth. Agencies then can work toward staying within the identified risk threshold and understand the impact if they must exceed that threshold.

2012 Risk Management Profile			
% of Business Impact Analysis Submitted	% of Agency Mission Essential Functions	% of Risk Assessment(s) Submitted	% of Threat Data Submitted
57 %	65%	50 %	86 %

Business Impact Analysis (BIA)

A BIA identifies essential business functions and assesses the impact to an agency’s mission if these functions are disrupted. The role of BIA in IT risk management is to identify the IT systems that support essential business functions. These IT systems must be designated as sensitive with respect to availability and protected accordingly. Of the 80 agencies, 46 (57 percent) submitted the required business impact analysis documentation. These BIAs indicated that 65 percent of the business functions using IT systems were considered mission essential.

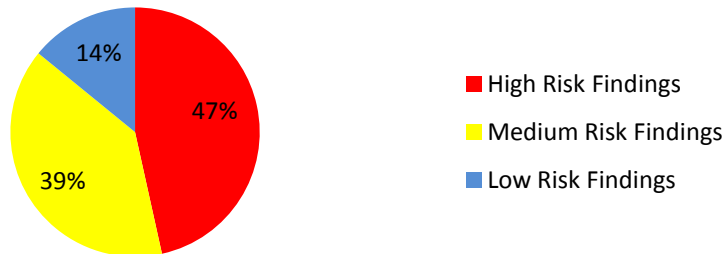
Risk Assessment

A risk assessment is the process of identifying vulnerabilities, threats, likelihood of occurrence, and potential loss or impact. Of the 80 agencies, 40 (50 percent) submitted the required risk assessment documents.

Risk Assessment Findings

Forty seven (47) percent of the findings reported on the risk assessments were high-risk findings, 39 percent were medium-risk findings and 14 percent were low-risk findings.

Risk Assessment Findings



Threat Metrics

A threat metric is a collection of threat information gathered by the agency based on attacks and attempted intrusions against agency information systems. These metrics allow CSRM to identify whether the risks that exist at an agency are being targeted for exploitation. CSRM then can ensure the agencies are prioritizing mitigation of these risks. Agencies that are part of the partnership have their threat metrics reported directly to CSRM on their behalf. Of the 80 agencies, 69 (86 percent) submitted the required threat metrics. Analysis of the submitted threat metrics is included in the Commonwealth Information Security Incident Management section of this report.

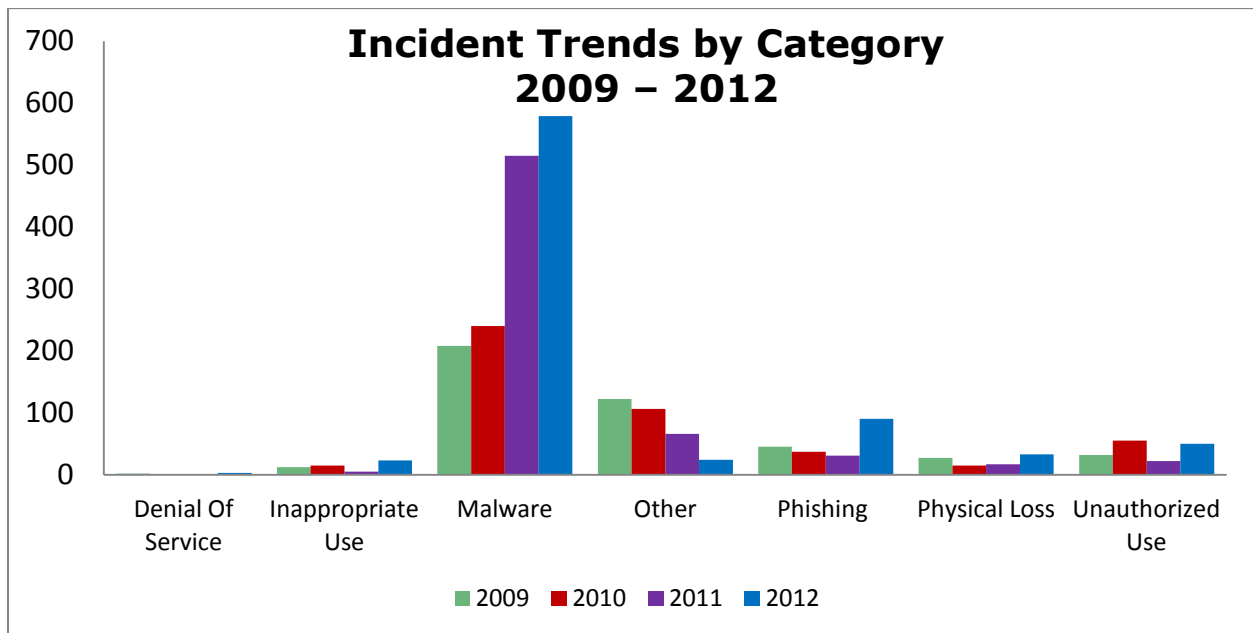
Commonwealth Cyber Threat and Attack Analysis

The *Code of Virginia, §2.2-603(F)*, requires all executive branch agency directors to report IT security incidents to the CIO within 24 hours of discovery. The Commonwealth Security Incident Response Team (CSIRT) categorizes each of these security incidents based on the type of activity.

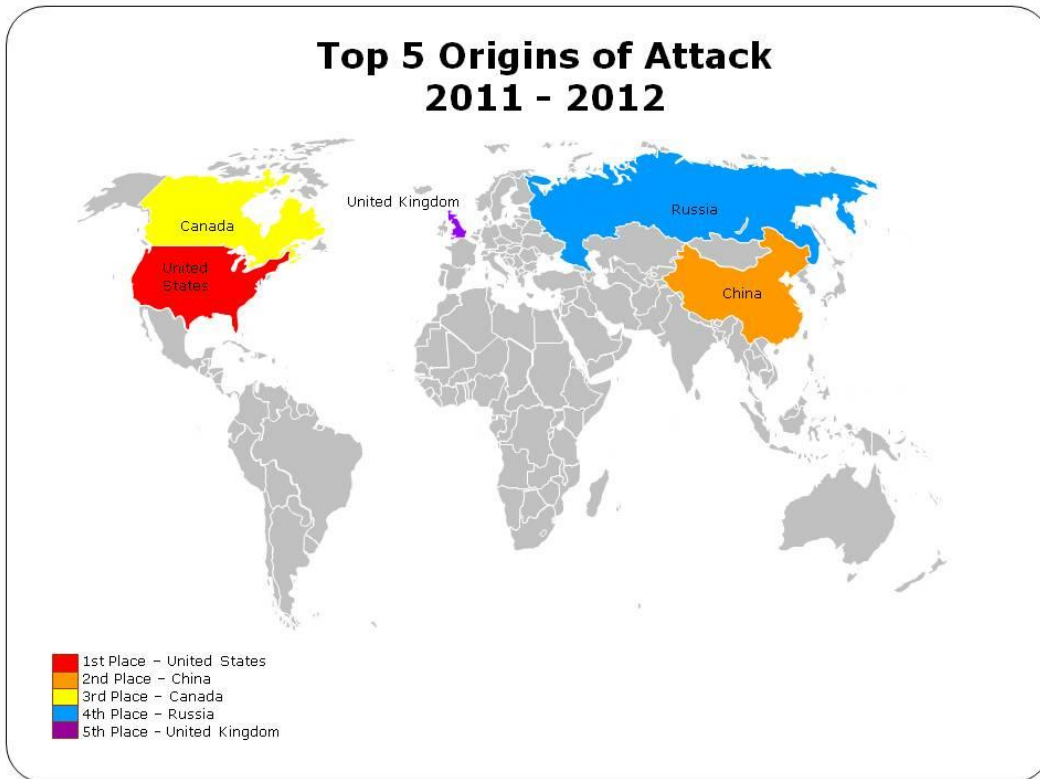
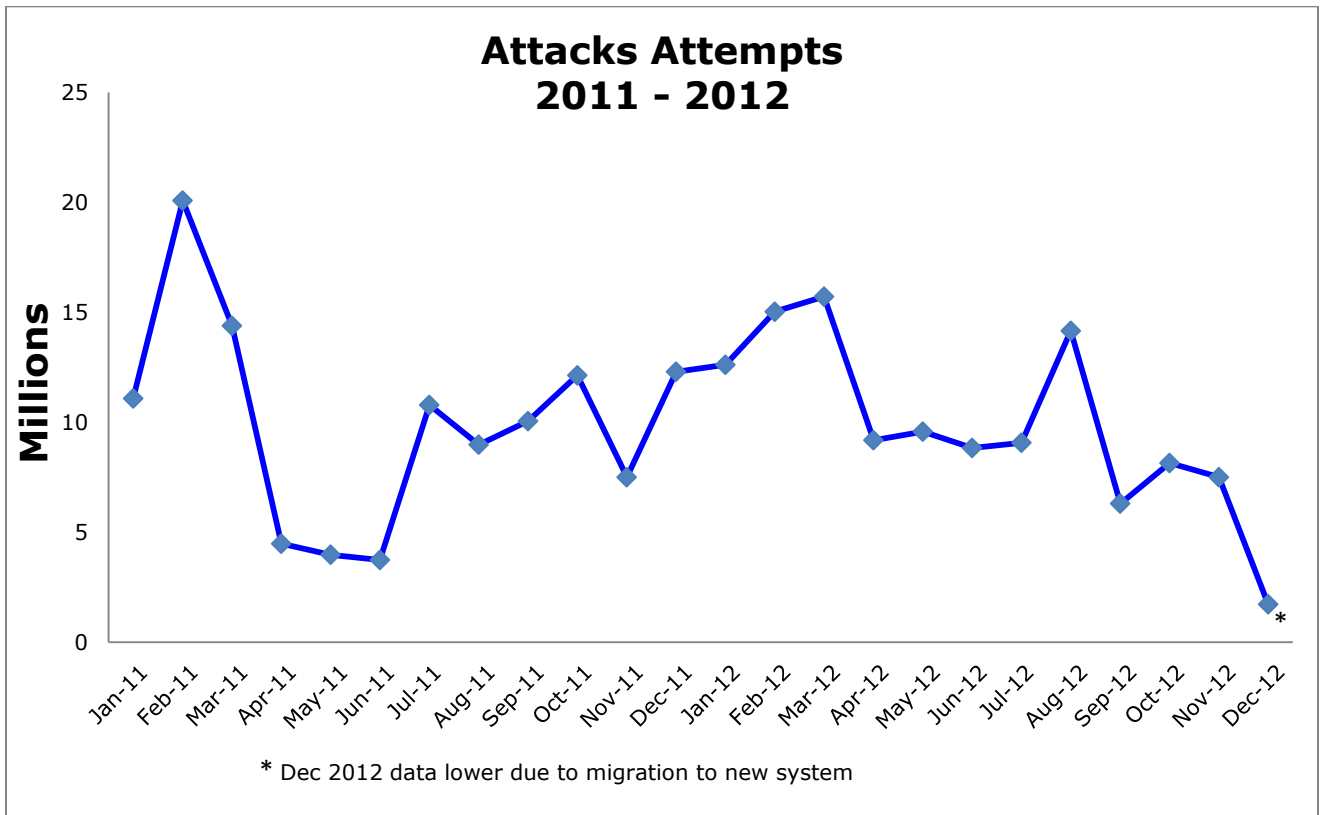
The data collected in 2012 shows that the Commonwealth continues to be a target for malicious attacks. This year reflected a significant increase – 21 percent – in the number of security incidents. While malware infections continued to be the top category for security incidents, there was a significant increasing in Phishing incidents. As users were tricked into giving up their credentials, the number of Authorized Accesses to COV systems increased. 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:

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

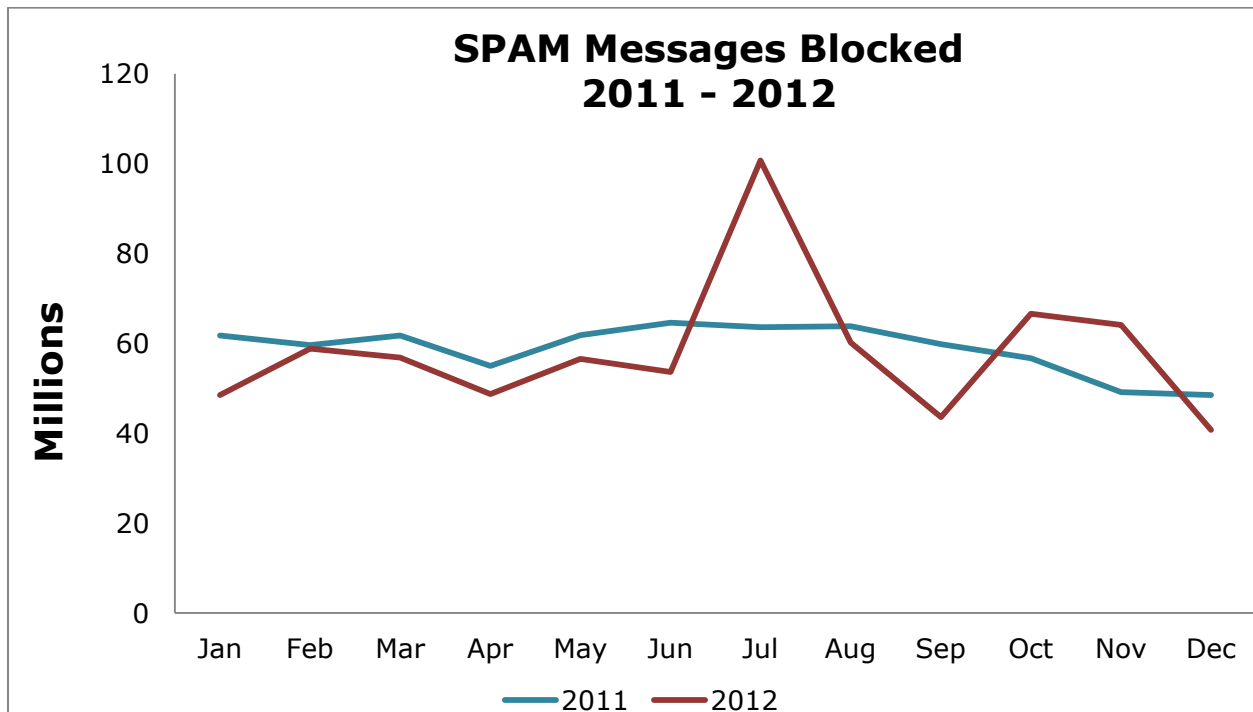


There are additional indicators of the size of the cyber threat to Virginia shown in the data collected from Virginia’s primary data center. The Commonwealth received 117,842,683 alerts, or approximately four attacks per second of malicious activity. While the vast majority of attacks were not successful, 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.

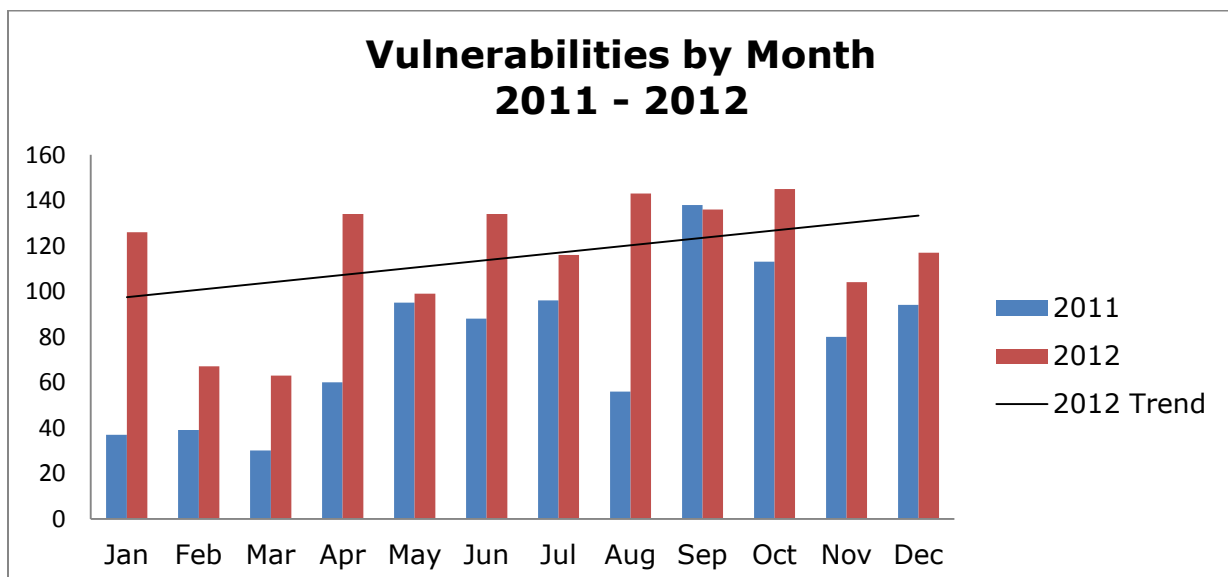


Email is a tool heavily utilized throughout the Commonwealth to carry out daily business. Security tools must be in place because of the heavy usage. Last year, the Commonwealth

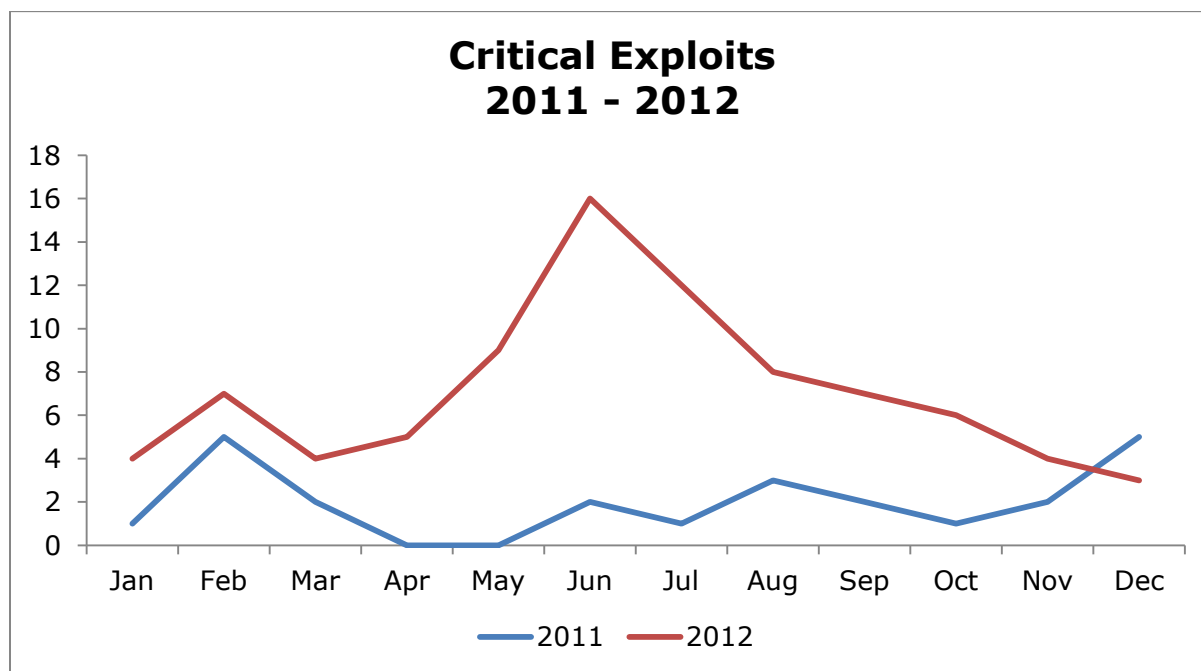
filtered 698,942,080 spam messages and blocked 47,698 viruses from reaching Commonwealth assets. Security personnel are constantly fine tuning the security environment to prevent unsolicited and malicious email from reaching the state employees' computers. As a result, users do not realize how much spam is blocked from their mailbox.



In an effort to foster security awareness, the security incident response team distributes a weekly advisory. This advisory contains information on new vulnerabilities that have been discovered in products that may be in use by state agencies and higher education. During 2012, the number of vulnerabilities being discovered increased each month, with an overall average increase of 150 percent for the year compared to 2011. The increase in vulnerabilities shows the issues that entities have with keeping systems secure.



Of the vulnerabilities that were reported, there was an increase of critical exploits, such as zero day exploits. In 2011, there were 24 critical exploits reported. In 2012, this number rose to 85. This is a 254 percent increase in critical exploits.



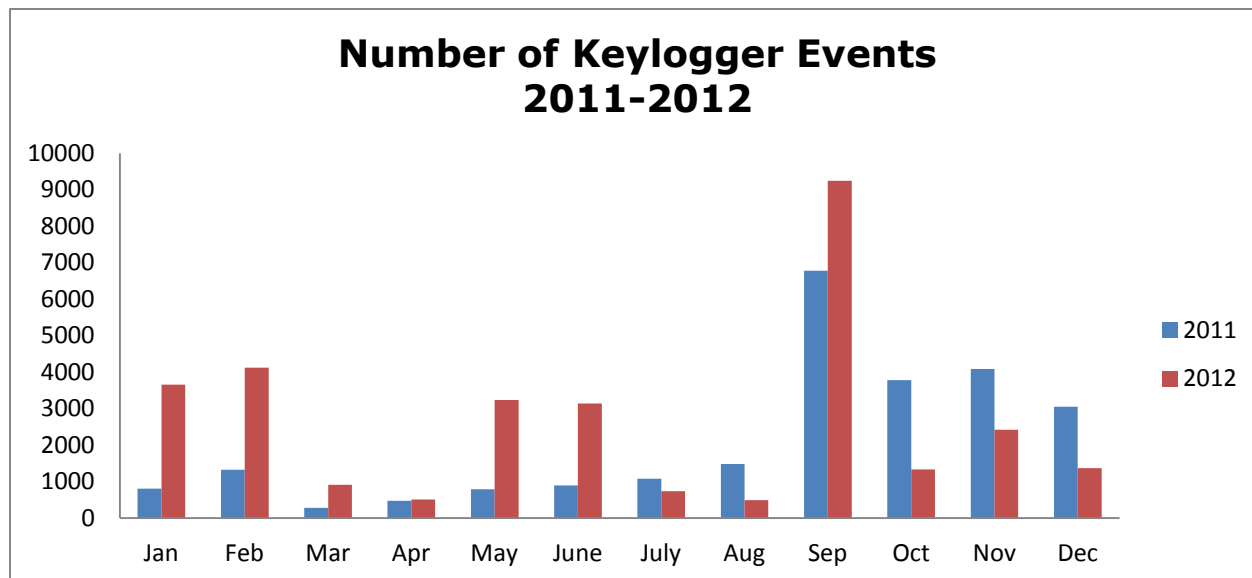
One of the additional services that the cyber security incident response program provides is gathering cyber intelligence information affecting the Commonwealth.

While a formal intelligence program is not funded, CSRM does 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 Virginia Fusion Center, Virginia State Police, Multi-State Information Analysis and Sharing Center (MS-ISAC), FBI, United States Computer Emergency Response Team and Department of Homeland Security. Information about security issues is regularly 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, 32 localities, 22 colleges and universities, and six public school systems to provide notifications of website defacements, compromised accounts and malware infections.

Because of the significant increase in cyber security incidents, CSRM recommends that the Commonwealth fund a cyber intelligence program through VITA. This program will provide analysis on threats and attempted attacks that are impacting the Commonwealth. A properly funded cyber intelligence program would provide two primary benefits. The first is insight for agency executives that will allow them to make risk-based decisions based on the likelihood of cyber attack attempts. The second benefit will allow the analysis of activity involving malicious third parties that are targeting the Commonwealth directly. CSRM has seen evidence of targeted attacks against the Commonwealth but up to this point has only been able to investigate individual security incidents. Formally funding a cyber intelligence program will help understand who is targeting the Commonwealth and why so that better security controls can be implemented.

The information received from Commonwealth partners includes data involving both state and local governments and 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 installed on a victim's system designed to record data transactions between the victim and a website or online service belonging to a state or local agency 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 2012, the Commonwealth experienced 31,187 keylogger events, a 24.9 percent increase over 2011. As a result of these events, personally identifiable information of 1,493 citizens was exposed.



Agency Information Security Program

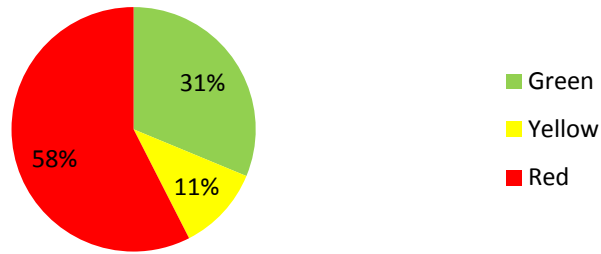
The Commonwealth’s IT Security and IT Security Audit Standards require that agencies develop and maintain an agency IT security program. Agencies are required to appoint a qualified Information Security Officer (ISO) and identify their sensitive systems, develop an IT security audit plan, conduct IT security audits on those systems at a minimum of every three years, and develop and maintain corrective action plans for findings.

In 2012, there was no noticeable improvement to the effectiveness of the agency IT security audit programs. The lack of progress continues to hinder an accurate assessment of the Commonwealth security program. However, CSRM has reviewed the information submitted and identified high-risk areas affecting the agencies. This information was provided to the agencies to make risk-based decisions on the allocation of resources within agencies’ information security program.

CSRM conducted two surveys of agency information security personnel to identify weaknesses in agency information security programs. The results identified a skill set gap in many agencies affecting designated information security personnel. In response to these results, CSRM is instituting an ISO certification program. The program will include required training courses specific to the Commonwealth security program and recognize industry certifications. Going forward, this report will indicate whether agencies have a certified ISO designated at the agency.

The ISO certification is intended to ensure that the designated ISO is familiar with the Commonwealth Information Security Program. Additionally, the certification requires training regarding industry IT security best practices. The training and certification is intended to increase the ability of agency ISOs to manage agency IT security programs and reduce risk to the agency. With the additional training, it is anticipated that the number of unresolved high-risk findings will decrease over the next three years.

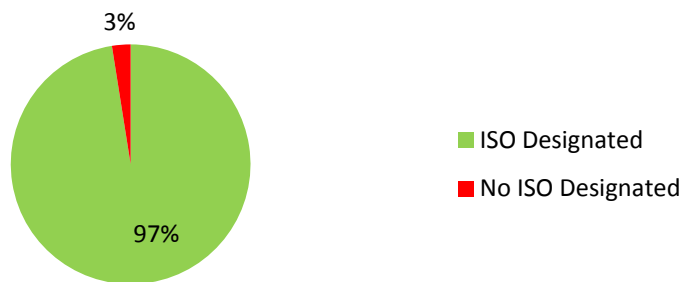
Commonwealth Overall Audit Program Score



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, implementing, and managing the agency’s IT security program.

Of the 80 agencies, 78 agencies (97 percent) have designated an ISO within the past two years.

ISO Designation



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 80 agencies, 43 agencies (54 percent) have sent a total of 83 persons to information security orientation, and 37 (46 percent) have not had a representative attend within the last two years.

Information Security Orientation

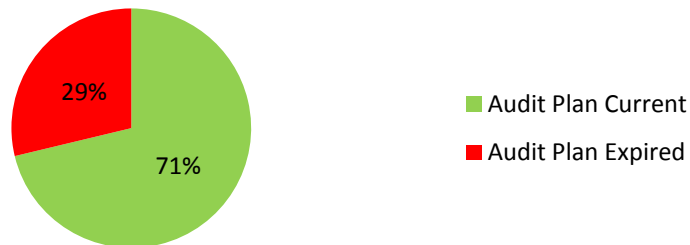


Information Security Officer Certification – Beginning in 2013, agency ISOs will be required to be certified to ensure that they have the necessary skill set to perform the job.

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 against 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. IT security audit plans help the agency schedule the necessary IT security audits of the sensitive systems identified in the risk management process. Each agency head must submit the agency IT security audit plan to the CISO annually.

Of the 80 agencies, 57 (71 percent) have submitted a current information security audit plan and 23 (29 percent) have an expired audit plan.

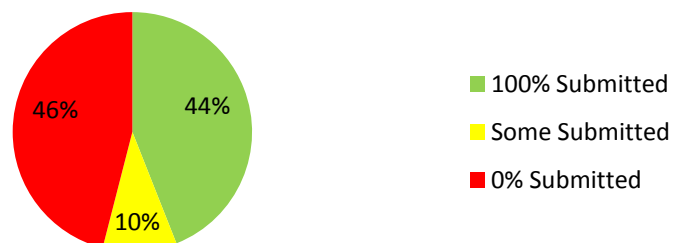
IT Security Audit Plan



Provide audit reports for complete information security audits - IT security audit reports document the results of the IT security audits. Audit results must be presented to the agency head or designee in a draft report for their review and comment. These results include IT security findings identified during the IT security audit and recommendations for remediation. IT security audit reports are required to be submitted to the CISO after the completion of a sensitive system IT security audit.

Of the 80 agencies, 50 agencies had sensitive system IT security audits scheduled for 2012. Of those agencies, 22 (44 percent) have submitted all IT security audit reports due; five (10 percent) have submitted some of the IT security audit reports due; and 23 (46 percent) have not submitted any of the IT security audit reports due.

Audit Reports

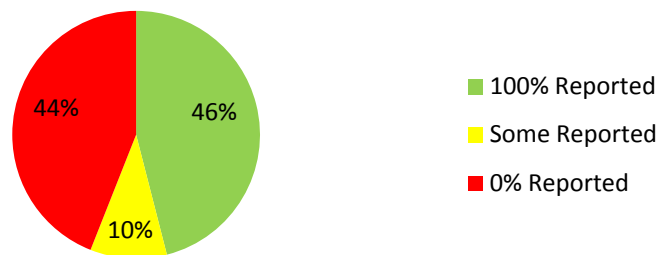


Provided corrective action plans for completed information security audits -

Corrective action plans are required to be submitted to the CISO each quarter to document IT security findings from the audits, whether the agency head agrees or disagrees with the audit findings, and, if in agreement, actions planned to correct the vulnerabilities identified. If the agency head disagrees with the finding, a statement of the agency’s position and acceptance of risk must be provided.

Of the 80 agencies, 50 agencies had sensitive system audits scheduled for 2012. Of those agencies, 23 (46 percent) have submitted all corrective action plans, or had no findings; five (10 percent) have submitted some corrective action plans; and 22 (44 percent) have not submitted any of the corrective action plans due in 2012.

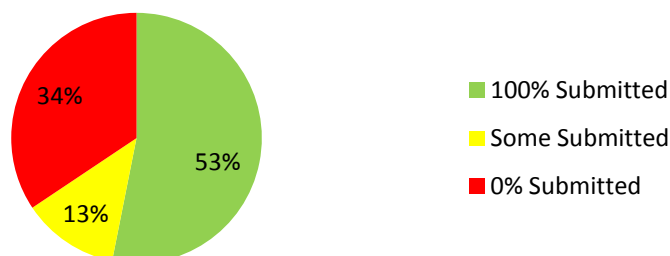
Corrective Action Plans



Supplied 2012 quarterly updates for open corrective action plans - In order to track the progress of remediation for submitted corrective action plans, agencies are required to provide quarterly updates of corrective action plans with open findings to the CISO. These updates contain the status of outstanding corrective actions and the expected completion date. The quarterly updates continue until the corrective actions have been completed.

Of the 80 agencies, 32 agencies had quarterly updates due for open corrective action plans in 2012. Of those 32 agencies, 17 (53 percent) have submitted all updates; four agencies (13 percent) have submitted some of the updates; and 11 agencies (34 percent) have not submitted any updates.

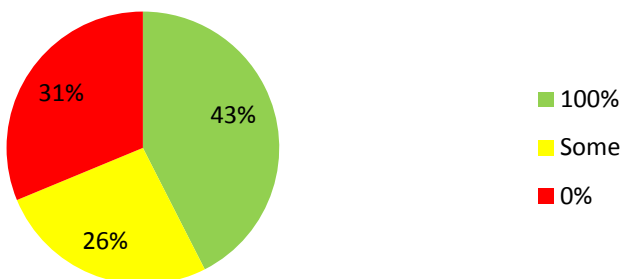
Quarterly Updates



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.

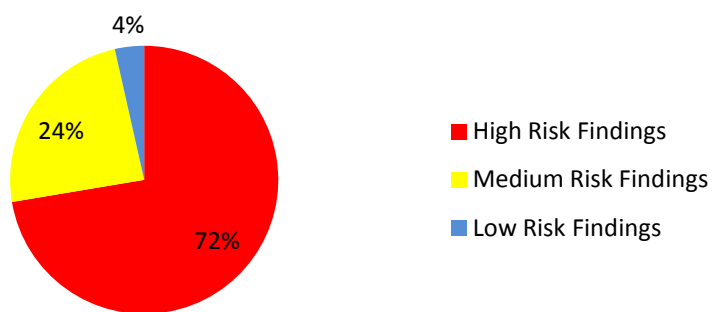
Of the 80 agencies, 34 (43 percent) have completely fulfilled the obligation to have every sensitive system audited at least once every three years, and 21 (26 percent) have partially completed their audit obligation. At the other end of the spectrum, 25 agencies (31 percent) have not performed any audits or have not submitted evidence of an audit for their systems in the last three years to the CISO.

Audit Obligation Completed



IT Security Audit Findings – in order to understand the risk that the Commonwealth is carrying, the unresolved audit findings have been classified as high, medium or low risk. At the end of 2012, 72 percent of the unresolved IT security audit findings were considered high risk, 24 percent were considered medium risk, and 4 percent were considered low risk.

IT Security Audit Findings



Methodology

The *2012 Annual Report on Information Security (IT) in the Commonwealth* builds on a baseline created in 2008 for assessing the strength of the information security programs that state agencies have established to protect Commonwealth information. The scope of this report is limited to the independent and executive branch agencies, including Tier III institutions of higher education. This report does not address charter and Tier II institutions that have been statutorily exempted from compliance with Commonwealth policies and standards.

This report is not based on field reviews of the information security programs at individual agencies, but rather on an analysis of data and information reported by these agencies to the CISO as of December 31, 2012. The COV Information Security Policy, Standard and Audit Standard requires that certain data be reported by agencies to the CISO, and that data serve 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 IT security audit reports
- Provided corrective action plans for completed information security audits
- Submitted IT security exceptions
- 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.)
- Submitted agency risk assessments
- submitted agency business impact analysis
- submitted agency threat metrics

The detailed listing of agencies and specific security data points can be found in the appendix. In addition, CSRM analyzed security incidents reported by executive branch agencies and utilized information from the Commonwealth IT infrastructure.



Appendix I - Agency Information Security Datapoints - Dashboard

Agency Information Security Datapoints Dashboard - Legend





ISO Designated

-  - The agency head has designated an Information Security Officer (ISO) for the agency within the past two years.
-  - The agency head has NOT designated an ISO for the agency within the past two years.




Attended ISO Certification

-  - The primary ISO is certified
-  - The primary ISO is NOT certified.

2012 Overall Audit Program

-  - Documents received as scheduled
-  - Missing corrective action plan(s) or quarterly update(s)
-  - Missing audit plan
-  - Have not met audit obligation

2012 Overall Risk Profile

-  - All documentation received as requested information about the agency's BIA, RA(s)¹ and IDS reports
-  - Missing IDS report(s)
-  - Missing any required documentation as requested information about the agency's BIA and RA(s)

Agency Information Security Datapoints - Dashboard

¹ Risk Assessment(s) for sensitive system(s) scheduled to be audited this calendar year

Secretariat	Agency Name	Agency Acronym	ISO Designated	2012 Overall Audit Program	Overall Risk Profile
Administration	Compensation Board	CB			
Administration	Department of General Services	DGS			
Administration	Department of Human Resource Management	DHRM			
Administration	Department of Minority Business Enterprise	DMBE			
Administration	Office of State Inspector General	OISG			
Administration	State Board of Elections	SBE			
Agriculture & Forestry	Department of Forestry	DOF			
Agriculture & Forestry	Department of Agriculture and Consumer Services	VDACS			
Commerce & Trade	Board of Accountancy	BOA			
Commerce & Trade	Department of Business Assistance	DBA			
Commerce & Trade	Department of Housing and Community Development	DHCD			
Commerce & Trade	Department of Mines, Minerals and Energy	DMME			
Commerce & Trade	Department of Labor and Industry	DOLI			
Commerce & Trade	Department of Professional & Occupational Regulation	DPOR			
Commerce & Trade	Tobacco Indemnification and Revitalization Commission	TIC			
Commerce & Trade	Virginia Employment Commission	VEC			
Commerce & Trade	Virginia Economic Development Partnership	VEDP			
Commerce & Trade	Virginia Resources Authority	VRA			
Commerce & Trade	Virginia Racing Commission	VRC			
Education	Department of Education	DOE			
Education	Frontier Culture Museum of Virginia	FCMV			
Education	Gunston Hall	GH			
Education	Jamestown-Yorktown Foundation	JYF			
Education	The Library of Virginia	LVA			
Education	Norfolk State University	NSU			
Education	Richard Bland College	RBC			
Education	State Council of Higher Education for Virginia	SCHEV			
Education	Science Museum of Virginia	SMV			

Secretariat	Agency Name	Agency Acronym	ISO Designated	2012 Overall Audit Program	Overall Risk Profile
Education	Southern Virginia Higher Education Center	SVHEC			
Education	University of Mary Washington	UMW			
Education	Virginia Commission for the Arts	VCA			
Education	Virginia Museum of Fine Arts	VMFA			
Education	Virginia School for the Deaf and Blind	VSDB			
Education	Virginia State University	VSU			
Executive	Office of the Governor	GOV			
Executive	Office of the Attorney General	OAG			
Finance	Department of Accounts	DOA			
Finance	Department of Planning and Budget	DPB			
Finance	Department of Taxation	TAX			
Finance	Department of the Treasury	TD			
H & HR	Comprehensive Services for At-Risk Youth & Families	CSA			
H & HR	Department of Behavioral Health and Developmental Services	DBHDS			
H & HR	Department of Health Professions	DHP			
H & HR	Department of Medical Assistance Services	DMAS			
H & HR	Department of Rehabilitative Services	DRS			
H & HR	Department of Social Services	DSS			
H & HR	Department of Health	VDH			
H & HR	Virginia Foundation for Healthy Youth	VFHY			
Independent	Indigent Defense Commission	IDC			
Independent	State Corporation Commission	SCC			
Independent	State Lottery Department	SLD			
Independent	Virginia Collage Savings Plan	VCSP			
Independent	Virginia Office for Protection and Advocacy	VOPA			
Independent	Virginia Retirement System	VRS			
Independent	Virginia Workers Compensation Commission	VWC			
Natural Resources	Department of Conservation and Recreation	DCR			

Secretariat	Agency Name	Agency Acronym	ISO Designated	2012 Overall Audit Program	Overall Risk Profile
Natural Resources	Department of Environmental Quality	DEQ			
Natural Resources	Department of Game and Inland Fisheries	DGIF			
Natural Resources	Department of Historic Resources	DHR			
Natural Resources	Marine Resources Commission	MRC			
Natural Resources	Virginia Museum of Natural History	VMNH			
Public Safety	Department of Alcoholic Beverage Control	ABC			
Public Safety	Commonwealths Attorneys Services Council	CASC			
Public Safety	Department of Criminal Justice Services	DCJS			
Public Safety	Department of Emergency Management	DEM			
Public Safety	Department of Fire Programs	DFP			
Public Safety	Department of Forensic Sciences	DFS			
Public Safety	Department of Juvenile Justice	DJJ			
Public Safety	Department of Military Affairs	DMA			
Public Safety	Department of Corrections	DOC			
Public Safety	Department of Veterans Services	DVS			
Public Safety	Department of State Police	VSP			
Technology	Innovation and Entrepreneurship Investment Authority	IEIA			
Technology	Virginia Information Technologies Agency	VITA			
Transportation	Department of Motor Vehicles	DMV			
Transportation	Department of Aviation	DOAV			
Transportation	Department of Rail and Public Transportation	DRPT			
Transportation	Motor Vehicle Dealer Board	MVDB			
Transportation	Department of Transportation	VDOT			
Transportation	Virginia Port Authority	VPA			

Appendix II - 2012 Overall Audit Program Scores

Legend

- **IT Security Audit Plan Received**

- **Current** - Submitted an IT Security Audit Plan for the period of fiscal year (FY) 2012-2014 or 2013-2015 for systems classified as sensitive based on confidentiality, integrity or availability (Note: After July 1, 2012, Audit Plans submitted shall reflect 2013-2015.)
- **Expired** - Submitted an IT Security Audit Plan on file that does not contain the current three year period fiscal year (FY) 2012-2014 or 2013-2015

- **Security Audit Reports Received**

- **X%** - The percentage of due audit reports received based on the security audit plan
- **N/A** - Not applicable as the agency had no audits due or the agency head has not submitted a security audit plan.

- **Audit Reports Received, Corrective Action Plans Received and Quarterly Updates Received**

- **X%** - The percentage of due corrective action plans and quarterly updated received based on the security audit plan
- **N/A** - Not applicable as the agency had no corrective action plans or quarterly updated due or the agency head has not submitted a security audit plan.

- **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.

Detailed Agency Information Security Datapoints - 2012 Overall Audit Program Scores

Secretariat	Agency Name	Agency Acronym	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
Administration	Compensation Board	CB	Current	0	0	N/A	0

Secretariat	Agency Name	Agency Acronym	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
Administration	Department of General Services	DGS	Current	0	0	0	25
Administration	Department of Human Resource Management	DHRM	Current	0	0	N/A	100
Administration	Department of Minority Business Enterprise	DMBE	Current	100	100	N/A	100
Administration	Office of State Inspector General	OISG	Expired	N/A	N/A	N/A	0
Administration	State Board of Elections	SBE	Expired	N/A	N/A	N/A	0
Agriculture & Forestry	Department of Forestry	DOF	Current	0	0	N/A	100
Agriculture & Forestry	Department of Agriculture and Consumer Services	VDACS	Current	100	100	100	100
Commerce & Trade	Board of Accountancy	BOA	Current	100	100	N/A	100
Commerce & Trade	Department of Business Assistance	DBA	Expired	N/A	N/A	N/A	0
Commerce & Trade	Department of Housing and Community Development	DHCD	Current	0	0	0	80
Commerce & Trade	Department of Mines, Minerals and Energy	DMME	Current	100	100	0	57
Commerce & Trade	Department of Labor and Industry	DOLI	Expired	0	0	N/A	0
Commerce & Trade	Department of Professional & Occupational Regulation	DPOR	Expired	N/A	N/A	25	100
Commerce & Trade	Tobacco Indemnification and Revitalization Commission	TIC	Expired	N/A	N/A	N/A	0
Commerce & Trade	Virginia Employment Commission	VEC	Current	100	100	100	56
Commerce & Trade	Virginia Economic Development Partnership	VEDP	Expired	0	0	N/A	0
Commerce & Trade	Virginia Resources Authority	VRA	Expired	N/A	N/A	N/A	0
Commerce & Trade	Virginia Racing Commission	VRC	Current	0	0	0	100
Education	Department of Education	DOE	Current	100	100	100	100
Education	Frontier Culture Museum of Virginia	FCMV	Current	N/A	N/A	N/A	100
Education	Gunston Hall	GH	Expired	N/A	N/A	N/A	0
Education	Jamestown-Yorktown Foundation	JYF	Current	0	0	N/A	100
Education	The Library of Virginia	LVA	Current	100	100	N/A	100
Education	Norfolk State University	NSU	Current	0	100	0	22
Education	Richard Bland College	RBC	Current	N/A	N/A	N/A	100
Education	State Council of Higher Education for Virginia	SCHEV	Expired	0	0	N/A	0
Education	Science Museum of Virginia	SMV	Current	N/A	N/A	N/A	100
Education	Southern Virginia Higher Education Center	SVHEC	Current	N/A	N/A	N/A	100

Secretariat	Agency Name	Agency Acronym	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
Education	University of Mary Washington	UMW	Current	100	100	33.33	100
Education	Virginia Commission for the Arts	VCA	Expired	0	0	N/A	100
Education	Virginia Museum of Fine Arts	VMFA	Current	0	0	0	0
Education	Virginia School for the Deaf and Blind	VSDB	Expired	0	0	N/A	0
Education	Virginia State University	VSU	Current	100	100	100	78
Executive	Office of the Governor	GOV	Current	0	0	N/A	0
Executive	Office of the Attorney General	OAG	Current	N/A	N/A	0	100
Finance	Department of Accounts	DOA	Current	0	0	100	25
Finance	Department of Planning and Budget	DPB	Expired	N/A	N/A	0	0
Finance	Department of Taxation	TAX	Current	36	36	100	58
Finance	Department of the Treasury	TD	Expired	0	0	N/A	0
H & HR	Comprehensive Services for At-Risk Youth & Families	CSA	Current	N/A	N/A	N/A	0
H & HR	Department of Behavioral Health and Developmental Services	DBHDS	Current	N/A	N/A	0	83
H & HR	Department of Health Professions	DHP	Current	N/A	N/A	N/A	100
H & HR	Department of Medical Assistance Services	DMAS	Current	100	100	N/A	98
H & HR	Department of Rehabilitative Services	DRS	Current	100	100	100	36
H & HR	Department of Social Services	DSS	Current	33	33	0	42
H & HR	Department of Health	VDH	Current	86	86	100	45
H & HR	Virginia Foundation for Healthy Youth	VFHY	Current	N/A	N/A	N/A	100
Independent	Indigent Defense Commission	IDC	Current	N/A	N/A	58.33	80
Independent	State Corporation Commission	SCC	Current	100	100	100	100
Independent	State Lottery Department	SLD	Current	100	100	45.45	50
Independent	Virginia Collage Savings Plan	VCSP	Current	100	100	N/A	100
Independent	Virginia Office for Protection and Advocacy	VOPA	Expired	N/A	N/A	N/A	0
Independent	Virginia Retirement System	VRS	Current	89	89	100	69
Independent	Virginia Workers Compensation Commission	VWC	Current	0	0	N/A	17
Natural Resources	Department of Conservation and Recreation	DCR	Current	0	0	0	100
Natural Resources	Department of Environmental Quality	DEQ	Current	N/A	N/A	N/A	67

Secretariat	Agency Name	Agency Acronym	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
Natural Resources	Department of Game and Inland Fisheries	DGIF	Current	N/A	N/A	N/A	100
Natural Resources	Department of Historic Resources	DHR	Current	100	100	N/A	100
Natural Resources	Marine Resources Commission	MRC	Current	N/A	N/A	N/A	100
Natural Resources	Virginia Museum of Natural History	VMNH	Expired	N/A	N/A	N/A	0
Public Safety	Department of Alcoholic Beverage Control	ABC	Current	100	100	100	86
Public Safety	Commonwealths Attorneys Services Council	CASC	Current	N/A	N/A	N/A	100
Public Safety	Department of Criminal Justice Services	DCJS	Expired	N/A	N/A	N/A	0
Public Safety	Department of Emergency Management	DEM	Current	0	0	N/A	0
Public Safety	Department of Fire Programs	DFP	Expired	0	0	N/A	0
Public Safety	Department of Forensic Sciences	DFS	Current	100	100	100	100
Public Safety	Department of Juvenile Justice	DJJ	Current	100	100	N/A	100
Public Safety	Department of Military Affairs	DMA	Expired	N/A	N/A	N/A	0
Public Safety	Department of Corrections	DOC	Current	100	100	100	100
Public Safety	Department of Veterans Services	DVS	Current	N/A	N/A	N/A	100
Public Safety	Department of State Police	VSP	Current	100	100	100	100
Technology	Innovation and Entrepreneurship Investment Authority	IEIA	Expired	0	0	N/A	0
Technology	Virginia Information Technologies Agency	VITA	Current	0	0	100	33
Transportation	Department of Motor Vehicles	DMV	Current	100	100	100	100
Transportation	Department of Aviation	DOAV	Current	100	100	N/A	100
Transportation	Department of Rail and Public Transportation	DRPT	Expired	N/A	N/A	N/A	0
Transportation	Motor Vehicle Dealer Board	MVDB	Expired	N/A	N/A	N/A	100
Transportation	Department of Transportation	VDOT	Current	86	86	100	96
Transportation	Virginia Port Authority	VPA	Expired	N/A	N/A	N/A	0

Appendix III - 2012 Complete Risk Profile IT Security Audit Findings

Detailed Agency Information Security Datapoints - 2012 Complete Audit Finding Risk Profile Totals

Legend

- Open High Risk Findings** - Percentage of open IT security audit findings rated as high risk
- Open Medium Risk Findings** - Percentage of open IT security audit findings rated as medium risk
- Open Low Risk Findings** - Percentage of open IT security audit findings rated as low risk

*Note: N/A indicates that the agency does not have any open IT security audit findings open according to documentation submitted to VITA.

Secretariat	Agency Name	Agency Acronym	Open High Risk Findings	Open Medium Risk Findings	Open Low Risk Findings
Administration	Compensation Board	CB	N/A	N/A	N/A
Administration	Department of General Services	DGS	100%	N/A	N/A
Administration	Department of Human Resource Management	DHRM	N/A	N/A	N/A
Administration	Department of Minority Business Enterprise	DMBE	N/A	N/A	N/A
Administration	Office of State Inspector General	OISG	N/A	N/A	N/A
Administration	State Board of Elections	SBE	N/A	N/A	N/A
Agriculture & Forestry	Department of Forestry	DOF	N/A	N/A	N/A
Agriculture & Forestry	Department of Agriculture and Consumer Services	VDACS	100%	0%	0%
Commerce & Trade	Board of Accountancy	BOA	N/A	N/A	N/A
Commerce & Trade	Department of Business Assistance	DBA	N/A	N/A	N/A
Commerce & Trade	Department of Housing and Community Development	DHCD	100%	N/A	N/A
Commerce & Trade	Department of Mines, Minerals and Energy	DMME	100%	N/A	N/A
Commerce & Trade	Department of Labor and Industry	DOLI	N/A	N/A	N/A
Commerce & Trade	Department of Professional & Occupational Regulation	DPOR	100%	N/A	N/A
Commerce & Trade	Tobacco Indemnification and Revitalization Commission	TIC	N/A	N/A	N/A
Commerce & Trade	Virginia Employment Commission	VEC	100%	0%	N/A
Commerce & Trade	Virginia Economic Development Partnership	VEDP	N/A	N/A	N/A

Secretariat	Agency Name	Agency Acronym	Open High Risk Findings	Open Medium Risk Findings	Open Low Risk Findings
Commerce & Trade	Virginia Resources Authority	VRA	N/A	N/A	N/A
Commerce & Trade	Virginia Racing Commission	VRC	100%	N/A	0%
Education	Department of Education	DOE	50%	N/A	20%
Education	Frontier Culture Museum of Virginia	FCMV	N/A	N/A	N/A
Education	Gunston Hall	GH	N/A	N/A	N/A
Education	Jamestown-Yorktown Foundation	JYF	N/A	N/A	N/A
Education	The Library of Virginia	LVA	N/A	N/A	N/A
Education	Norfolk State University	NSU	N/A	N/A	N/A
Education	Richard Bland College	RBC	N/A	N/A	N/A
Education	State Council of Higher Education for Virginia	SCHEV	N/A	N/A	N/A
Education	Science Museum of Virginia	SMV	N/A	N/A	N/A
Education	Southern Virginia Higher Education Center	SVHEC	N/A	N/A	N/A
Education	University of Mary Washington	UMW	N/A	N/A	N/A
Education	Virginia Commission for the Arts	VCA	N/A	N/A	N/A
Education	Virginia Museum of Fine Arts	VMFA	33%	N/A	N/A
Education	Virginia School for the Deaf and Blind	VSDB	N/A	N/A	N/A
Education	Virginia State University	VSU	42%	8%	8%
Executive	Office of the Governor	GOV	N/A	N/A	N/A
Executive	Office of the Attorney General	OAG	N/A	N/A	N/A
Finance	Department of Accounts	DOA	N/A	N/A	N/A
Finance	Department of Planning and Budget	DPB	N/A	N/A	N/A
Finance	Department of Taxation	TAX	93%	71%	0%
Finance	Department of the Treasury	TD	N/A	N/A	N/A
H & HR	Comprehensive Services for At-Risk Youth & Families	CSA	N/A	N/A	N/A
H & HR	Department of Behavioral Health and Developmental Services	DBHDS	0%	N/A	N/A
H & HR	Department of Health Professions	DHP	N/A	N/A	N/A
H & HR	Department of Medical Assistance Services	DMAS	N/A	N/A	N/A
H & HR	Department of Rehabilitative Services	DRS	32%	N/A	N/A

Secretariat	Agency Name	Agency Acronym	Open High Risk Findings	Open Medium Risk Findings	Open Low Risk Findings
H & HR	Department of Social Services	DSS	0%	1%	0%
H & HR	Department of Health	VDH	15%	N/A	N/A
H & HR	Virginia Foundation for Healthy Youth	VFHY	N/A	N/A	N/A
Independent	Indigent Defense Commission	IDC	100%	N/A	N/A
Independent	State Corporation Commission	SCC	100%	N/A	N/A
Independent	State Lottery Department	SLD	100%	N/A	N/A
Independent	Virginia Collage Savings Plan	VCSP	N/A	N/A	N/A
Independent	Virginia Office for Protection and Advocacy	VOPA	N/A	N/A	N/A
Independent	Virginia Retirement System	VRS	100%	N/A	N/A
Independent	Virginia Workers Compensation Commission	VWC	N/A	N/A	N/A
Natural Resources	Department of Conservation and Recreation	DCR	100%	N/A	N/A
Natural Resources	Department of Environmental Quality	DEQ	N/A	N/A	N/A
Natural Resources	Department of Game and Inland Fisheries	DGIF	N/A	N/A	N/A
Natural Resources	Department of Historic Resources	DHR	N/A	N/A	N/A
Natural Resources	Marine Resources Commission	MRC	N/A	N/A	N/A
Natural Resources	Virginia Museum of Natural History	VMNH	N/A	N/A	N/A
Public Safety	Department of Alcoholic Beverage Control	ABC	100%	N/A	N/A
Public Safety	Commonwealths Attorneys Services Council	CASC	N/A	N/A	N/A
Public Safety	Department of Criminal Justice Services	DCJS	N/A	N/A	N/A
Public Safety	Department of Emergency Management	DEM	N/A	N/A	N/A
Public Safety	Department of Fire Programs	DFP	N/A	N/A	N/A
Public Safety	Department of Forensic Sciences	DFS	60%	33%	0%
Public Safety	Department of Juvenile Justice	DJJ	N/A	N/A	N/A
Public Safety	Department of Military Affairs	DMA	N/A	N/A	N/A
Public Safety	Department of Corrections	DOC	100%	0%	0%
Public Safety	Department of Veterans Services	DVS	N/A	N/A	N/A
Public Safety	Department of State Police	VSP	100%	0%	0%
Technology	Innovation and Entrepreneurship Investment Authority	IEIA	N/A	N/A	N/A
Technology	Virginia Information Technologies Agency	VITA	100%	0%	0%

Secretariat	Agency Name	Agency Acronym	Open High Risk Findings	Open Medium Risk Findings	Open Low Risk Findings
Transportation	Department of Motor Vehicles	DMV	85%	2%	0%
Transportation	Department of Aviation	DOAV	N/A	N/A	N/A
Transportation	Department of Rail and Public Transportation	DRPT	N/A	N/A	N/A
Transportation	Motor Vehicle Dealer Board	MVDB	N/A	N/A	N/A
Transportation	Department of Transportation	VDOT	100%	0%	0%
Transportation	Virginia Port Authority	VPA	N/A	N/A	N/A