Virginia Information Technologies Agency

2014 Commonwealth of Virginia Information Security Report

www.vita.virginia.gov

Prepared and Published by:

Virginia Information Technologies Agency

Comments on the
2014 Commonwealth of Virginia Information Security Report
are welcome
Suggestions may be conveyed electronically to
CommonwealthSecurity@vita.virginia.gov

Please submit written correspondence to:

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

2014 Information Security Report

Executive Summary

This 2014 Commonwealth of Virginia (COV) Information Security Report is the seventh 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 annually 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 the six independent and 70 executive branch agencies, including the two Tier I institutions of higher education. This report does not address Tier III and Tier II institutions statutorily exempted from compliance with Commonwealth policies and standards.

The CIO has established a Commonwealth Security and Risk Management (CSRM) directorate within the Virginia Information Technologies Agency (VITA) to fulfill his information security duties under §2.2-2009. 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 the 76 agencies assessed in this report, and their specific security information concerns, can be found in the appendix.

Phishing attacks directly targeted the Commonwealth and affected over a quarter of all agencies. The Commonwealth has recently been targeted by malicious third parties with a series of emails intended to capture employee usernames and passwords. Commonwealth employees frequently fall victim to this type of cyberattack. Phishingattacks made up 31 percent of all reported incidents in 2014. Measures have been taken to reduce those attacks, but phishing is a continuing challenge in 2015, with phishing incidents rising to 35 percent of all incidents in the first quarter.

A timely scam promising a low interest rate on a loan hit the Commonwealth before Christmas and managed to snare hundreds of employees eager for extra holiday spending money. While information regarding these scams has been provided to employees, many users continue to provide credentials and other information.

Conversely, there is a contingent of Commonwealth employees who remain vigilant and report suspicious emails which is very helpful in containing the damage. In order to enhance prevention, CSRM is investigating new approaches to employee training, additional security controls, and other methods of encouraging the correct user behavior.

Agencies must identify funding to perform required security reviews of their sensitive IT systems. Fourteen additional sensitive systems were placed in service by agencies in 2014. For the past four years, the majority of agencies have failed to meet the minimum requirements for reviewing their sensitive systems. Agencies have been issued

notices informing them that their information security programs are not in compliance and that measures to reduce IT project spending will have to be taken until funds have been set aside for the necessary sensitive system reviews. VITA will be investigating the possibility of centrally implementing third-party security audits for non-compliant agencies if corrective measures are not taken.

Access control continues to be a significant area of weakness for the Commonwealth. Access control risks are responsible for 31 percent of all security audit findings and 22 percent of all security exception requests. Access control risk is becoming more widely uncovered throughout the Commonwealth. Agencies with access control findings increased 14 percent, with 69 percent of all agencies that submitted audits reporting at least one access control-related finding. To aid agencies in dealing with this issue, VITA has developed a template titled "Logical Access Controls Policy" to give additional guidance on how to check for and implement these controls. In addition, VITA will continue to work toward creating a security standard for identity access management.

The Commonwealth took steps to protect against the most dangerous software vulnerabilities of 2014. Several of these vulnerabilities took advantage of OpenSSL, which affects about 2/3 of all Web servers. Swift action was taken to ensure the Commonwealth was protected and patches were administered before the vulnerable devices could be compromised.

In 2014, Commonwealth agencies continued to lay the foundation for their risk programs. Requirements for this young program increased this year, with agencies expected to do more thorough reporting on threat data, vulnerability scanning, and risk assessment planning. Maturity was evident in the quality of the business impact analysis (BIA) submissions, for which there was a 23 percent reduction in incomplete submissions.

The Commonwealth's information security officer (ISO) certification program continues to grow. Eighty-six percent of the designated primary ISOs established a common educational background in information security specific to the Commonwealth. ISO certification is a leading indicator of whether or not an agency will have an adequate information security program. The education of these security professionals is vital to the success of their agency security programs. VITA will assess whether a requirement that ISOs hold a professional information security certification will keep the Commonwealth in line with best practices.

Commonwealth Operational Security

Operational security activities include those parts of the overall information security program that address and remediate threats and vulnerabilities within agency environments. To assess the overall threat posture, CSRM collects information from both the VITA IT infrastructure program as well as agencies falling outside the scope of the IT infrastructure program. This information is analyzed on a recurring basis in order to identify threats affecting the Commonwealth and identify widespread vulnerabilities.

Higher Risks to Commonwealth from IT Outside of Enterprise Framework

Certain areas of the Commonwealth's IT are either not protected by the enterprise security controls provided by VITA's infrastructure program, or are not subject to the same degree of oversight and reporting that governs enterprise infrastructure. These gaps need to be addressed through an appropriate use of enterprise protections for untransformed agencies and improved reporting for agency-specific IT and at higher education institutions.

Non-transformed agencies remain at significant operational security risk and cannot be adequately secured. The three "untransformed" agencies remain in an insecure state and are at a substantially elevated risk for intrusion, compromise and disruption: the Virginia State Police (VSP), the Virginia Department of Emergency Management (VDEM), and the Virginia Employment Commission (VEC). These agencies operate outside the enterprise security infrastructure and are vulnerable to attacks that would otherwise be mitigated by monitoring, intrusion detection, firewalls, encryption, virtual private networks (VPN) and other enterprise tools and resources. Risks are increasing as software goes out of date and new applications are put into production. These agencies need to complete transformation as soon as possible. If transformation is not completed, it is highly likely to cost each agency a significant amount of additional resources to have equivalent enterprise security controls put in place. Additionally, should those agencies attempt to implement the necessary enterprise security controls, the amount of risk incurred warrants an acceptance of risk from the corresponding secretary of each agency.

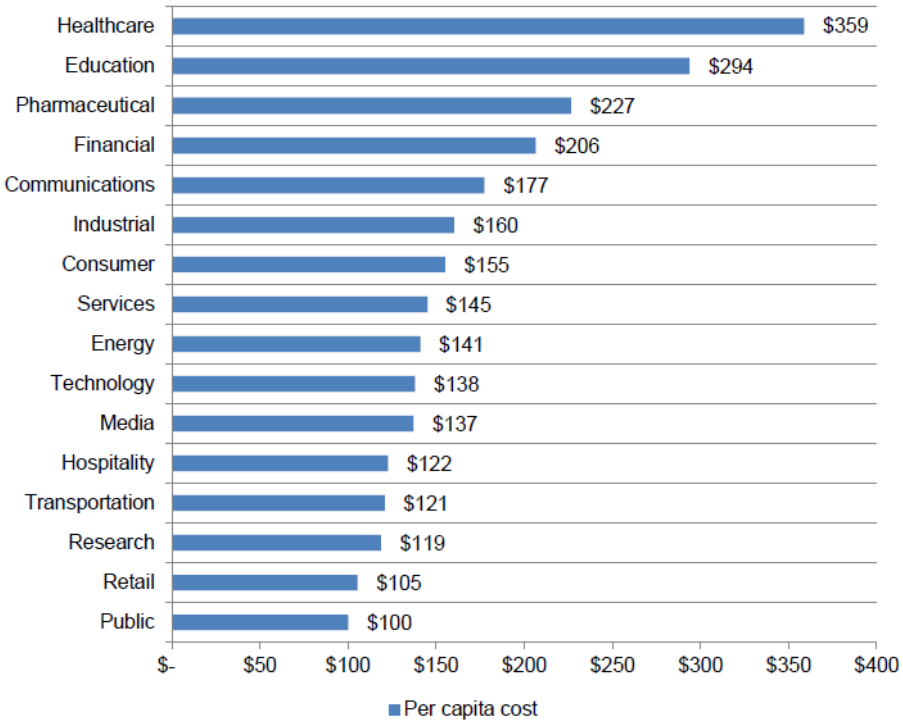
While two of the non-transformed agencies appear to be making progress, VSP has not yet shown significant progress toward transformation. The Auditor of Public Accounts has noted this lack of progress as an issue, as have VITA and specifically CSRM. VSP maintains a high level of inherent risk due to their mission and impact to life and safety. However, due to the lack of integration into the VITA program, VSP does not meet the standard security baseline applied to the rest of the executive branch. In order to ensure that the appropriate security controls are in place and that VSP utilizes existing security infrastructure rather than expending additional funds to duplicate an environment, CSRM recommends that VSP integrate into the enterprise environment as soon as possible.

Agency Control Systems, including Supervisory Control and Data Acquisition Systems, are not protected by enterprise security services. Historically, agencies typically have not protected agency-specific IT systems to the same degree as VITA's enterprise infrastructure, thus putting parts of the Commonwealth's overall infrastructure at risk. This elevated level of risk is of particular concern for Supervisory Control and Data Acquisition (SCADA) networks, also known as control systems, which contain computers and applications that support critical infrastructure. Examples of control systems include traffic control systems and health monitoring equipment. As additional control systems are used by agencies, it will be necessary to ensure a security baseline and effective security measures are applied to protect them. This is especially important for agency-specific systems that support critical infrastructure. Hampton Roads serves as an example of an area where compromises to the IT infrastructure that supports bridges and tunnels could cripple the local area. In order to ensure the necessary controls, an inventory of IT systems supporting critical infrastructure systems needs to be reported by agencies to CSRM so that this risk can be better evaluated and addressed.

Cyberattacks and other incidents at Virginia colleges and universities remain a significant risk. One of Virginia's greatest assets is the number of strong public higher education institutions. In addition to graduating educated professionals, these institutions also produce significant and valuable intellectual property. When the intellectual property at higher education institutions is combined with the number of confidential student, faculty and other sensitive records, these institutions become attractive targets for malicious third parties.

The Multi-State Information Sharing and Analysis Center sent out as many alerts for comprised higher education accounts as they did for all other forms of government combined (local government, public school systems, and state agencies). Not only do these

institutions account for a significant number of Commonwealth incidents, but as reported by the Ponemon Institute (below) the education sector has the second most costly breaches. (The Ponemon Institute is a research center dedicated to privacy, data protection and information security policy.)



Cyberattacks and other incidents at Virginia colleges and universities remain a significant risk to the Commonwealth due to the valuable intellectual property and confidential information at stake. Higher education institutions have a substantial amount of sensitive data related to functions and resources necessary to run their organizations' public safety, law enforcement functions, health facilities, health information systems, payment card processing, intellectual property, student personal information and financial systems. In order to properly protect the data in these institutions, robust information security programs are needed.

In Virginia, Tier II and III institutions with management agreements are statutorily exempt from VITA's oversight, but they still are required to develop and adopt their own IT security policies and standards. In practice, the management agreements have resulted in a lack of insight by VITA regarding the security policies and practices at covered institutions and the extent to which security incidents (including data breaches) occur. CSRM recommends that a standard set of governance requirements be established for these agencies, and that the institutions be required to report on metrics similar to the ones used in this annual report. Furthermore, we recommend legislation be introduced that will identify the parties responsible for evaluating the information security program at Tier II and III higher education institutions.

Improved Commonwealth Cyber Threat and Attack Analysis in 2014

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.

In 2014 the Commonwealth improved its IT security and risk analytics reporting through customization of a centralized governance and compliance system. Use of this system has allowed CSRM to correlate self-reported data from agencies across the Commonwealth, thereby providing a much clearer view of the systemic security problems and risks that need to be addressed. Agency auditors and ISOs soon will be asked to log directly into this system to securely attach items such as their audit plans, audit reports, corrective action plans and quarterly updates. This approach better positions the Commonwealth to be proactive about security by quickly identifying and remediating a risk before a breach occurs.

The data collected in 2014 shows that while the Commonwealth continues to be a target of attack, through the use of specific remediation efforts the overall number of incidents decreased by 58 percent. In the first three quarters of the year, the total number of incidents remained at close to the same level as in the fourth quarter of 2013 alone. The initial decrease during the first three quarters shows the continued coordinated enterprise-wide approach was a success.

Although the number of incidents has decreased, the number of incidents (262) in 2014 still remains a concern. Moreover, incident numbers from the fourth quarter show new attack vectors are being deployed against Commonwealth users and systems. While malware infections continued to be the top category for security incidents, there was a significant increase in unauthorized access due to users giving up their credentials via a phishing attack.

Phishing Attacks Involved Use of Outlook Web App

The increase in unauthorized access was evident during the fourth quarter when the Commonwealth came under a continuous phishing attack that lasted for several weeks. The concerted attack resulted in the number of incidents more than doubling from the previous quarter.

After much research, it was determined that the attackers were using Outlook Web App (OWA) to send the malicious emails from the compromised accounts. In order to reduce the impact of phishing attacks on the Commonwealth, CSRM has begun taking steps to implement two-factor authentication for remote access of systems, where possible. Two-factor authentication helps reduce the impact of users whose credentials are exposed to unauthorized third parties since it requires a combination of a password and something a user possesses to access systems.

In addition to two-factor authentication, CSRM is evaluating options to protect OWA from being used to send spam/phishing messages from compromised accounts. These options include moving OWA behind the VPN and requiring users to use a Commonwealth asset to access OWA. While CSRM understands that this will be an expense to agencies who normally allow users to connect using non-Commonwealth assets, this does follow best practices and protects Commonwealth systems from being exposed to malware residing on non-Commonwealth devices.

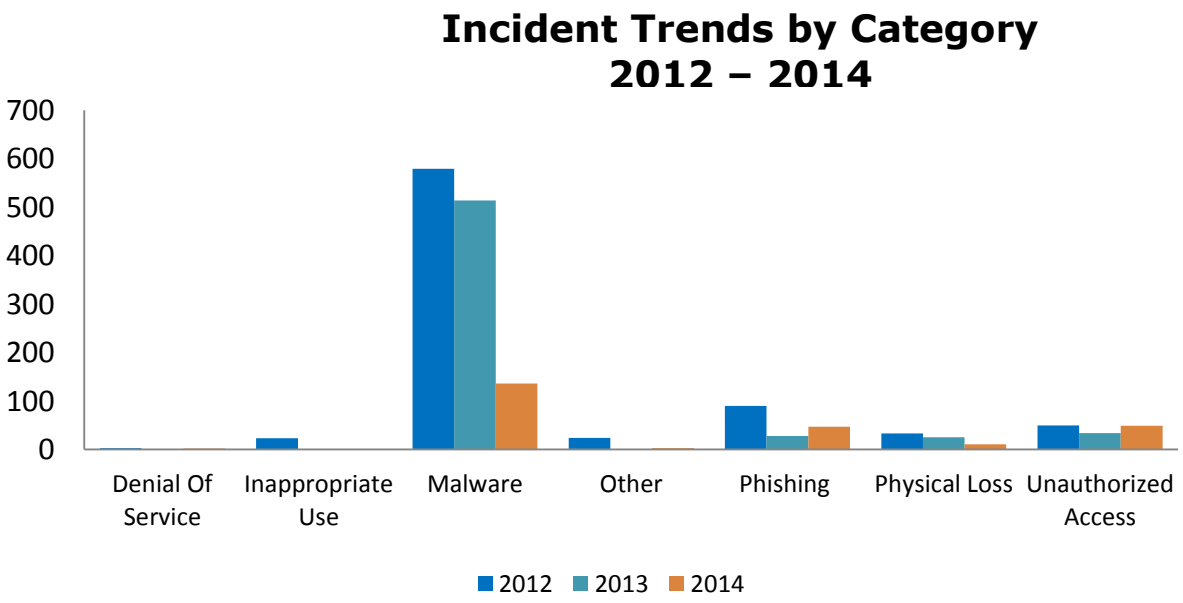
A direct correlation can be seen between the number of phishing attacks and the number of unauthorized access incidents. A phishing incident during the fourth quarter showed more sophistication than was previously seen. The attackers used the compromised account to send phishing messages to other Commonwealth users. Since the message was being sent

internally within the mail system, the emails were not scanned for spam and phishing characteristics. In addition, the COV users were more apt to fall for the phish as it appeared to be from a trusted source. This indicates that additional security awareness training is required as new attack vectors are discovered.

Incident Trends by Category

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

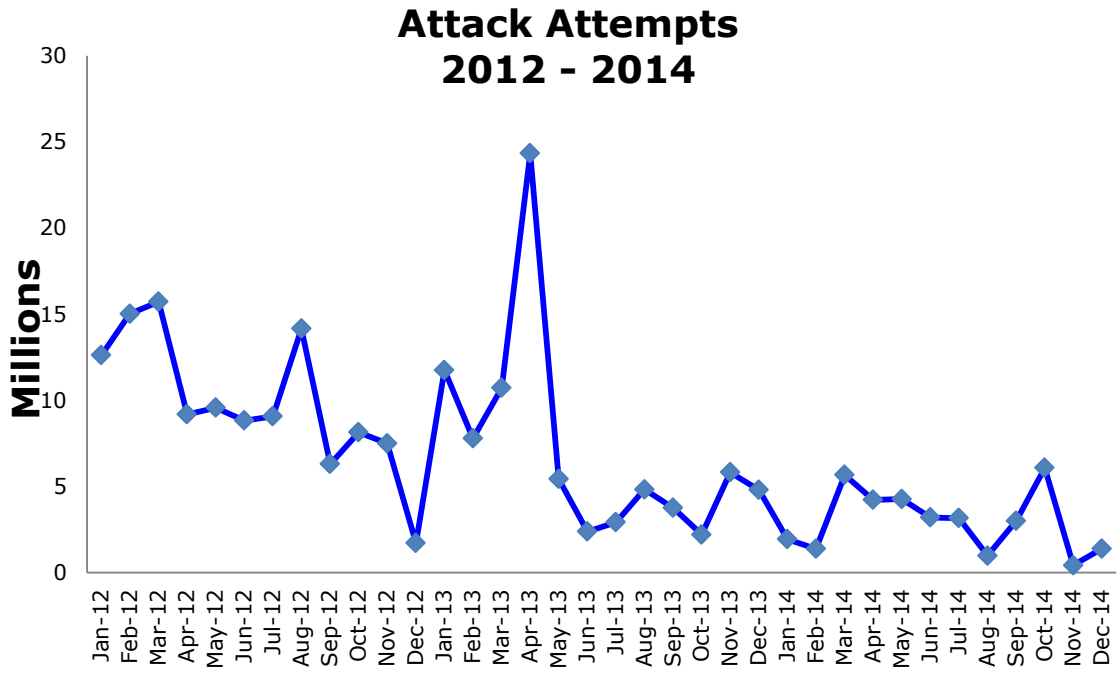
- Denial of service - Loss of availability of a COV service due to malicious activity
- Inappropriate usage - Misuse of COV resources
- Malware - Execution of malicious code such as viruses, spyware and key loggers
- Other - Reports where the investigation determines the event is not a security incident
- Phishing - Theft or attempted theft of user information such as account credentials
- Physical loss - Loss or theft of any COV resource that contains COV data
- 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.)



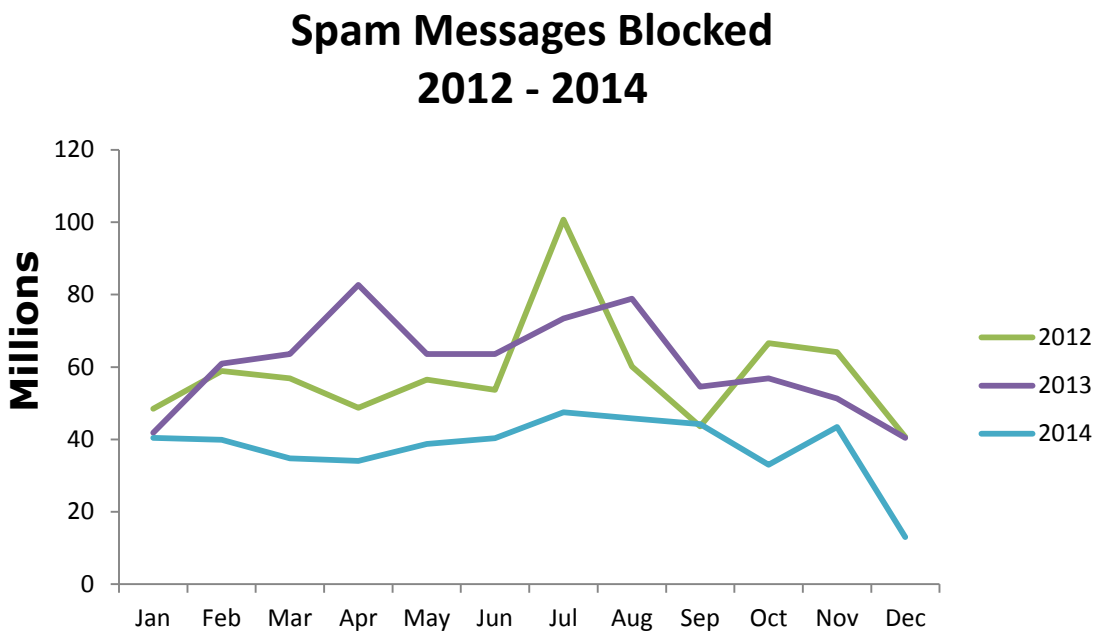
Note Use of compromised credentials in any attack, is categorized as Unauthorized Access.

There are additional indicators of the size of the cyberthreat to Virginia shown in the data collected from Virginia's primary data center. The Commonwealth received 35,761,877 alerts, or approximately one attack per second. While the vast majority of attacks were not successful, the number of attack attempts continually challenges Commonwealth IT security

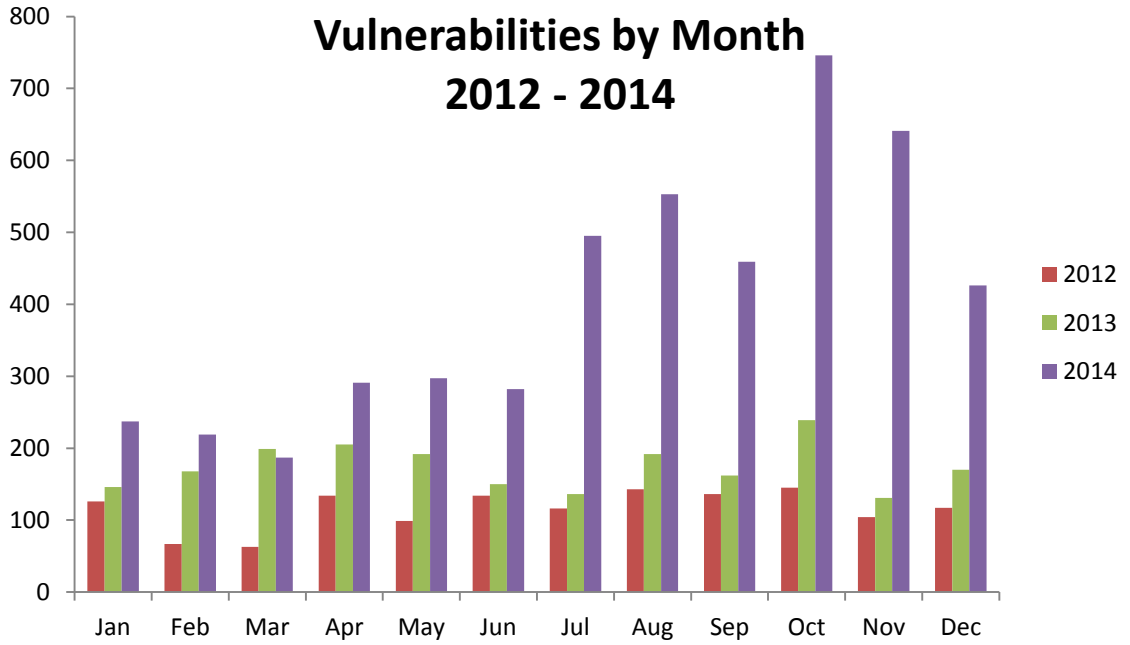
personnel to adapt quickly and defend against the constantly shifting cyberthreat in order to prevent data compromise.



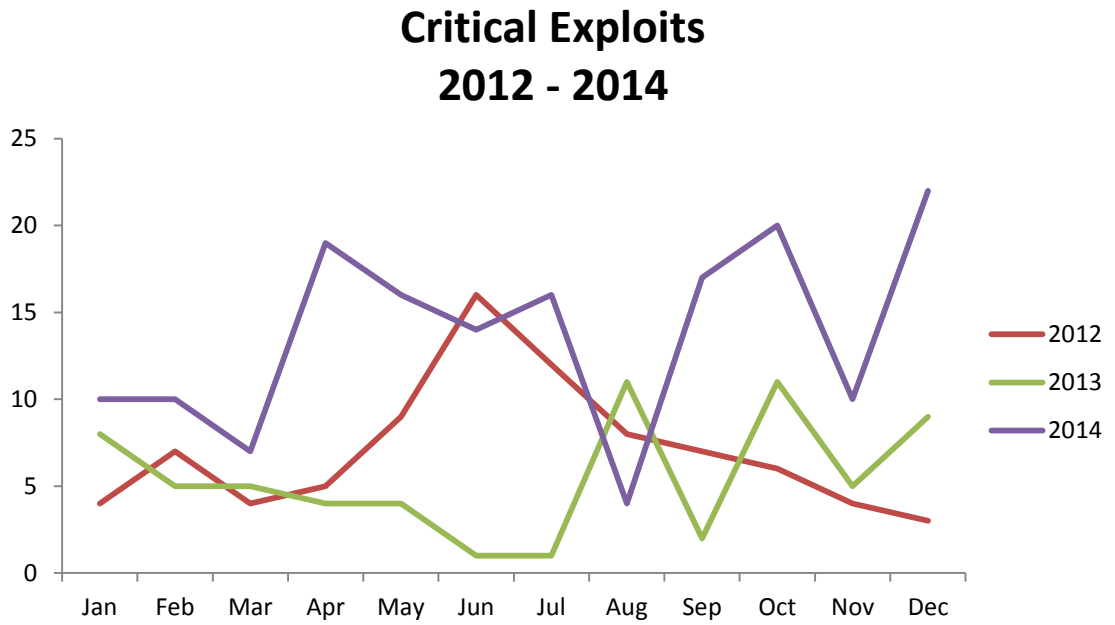
Email is utilized heavily throughout the Commonwealth to carry out daily business. Security tools must be in place because of the heavy usage. Last year, the Commonwealth filtered 455,117,558 spam messages and blocked 57,709 viruses from reaching Commonwealth assets. Security personnel are constantly fine-tuning the security environment to prevent unsolicited and malicious email from reaching state employee computers. As a result of this protection, users are unaware of how much spam is blocked from their mailboxes.



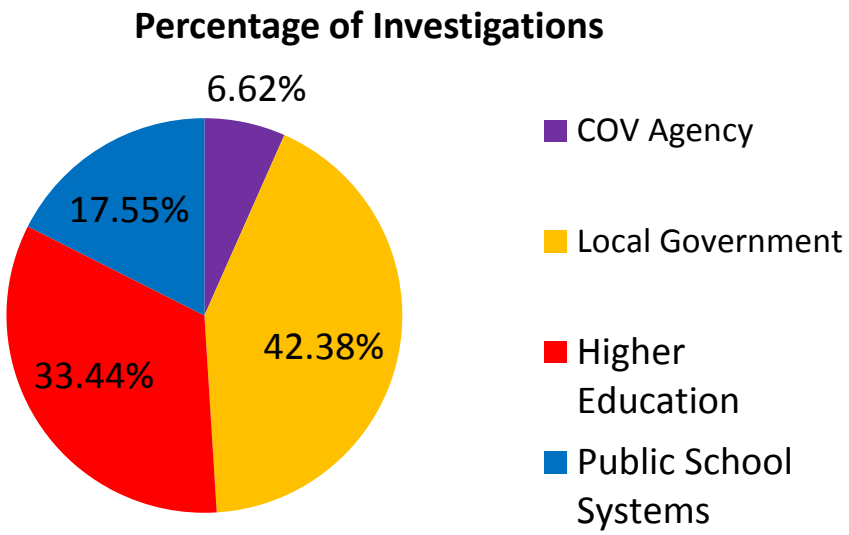
In an effort to foster security awareness, the security incident response team distributes a weekly advisory. This advisory contains information on new vulnerabilities that have been discovered in products that may be in use by state agencies and higher education. During 2014, the number of discovered vulnerabilities increased each month; for the year, the number increased on average by 231 percent over 2013. The increase in vulnerabilities shows the challenges agencies must face to keep systems secure.

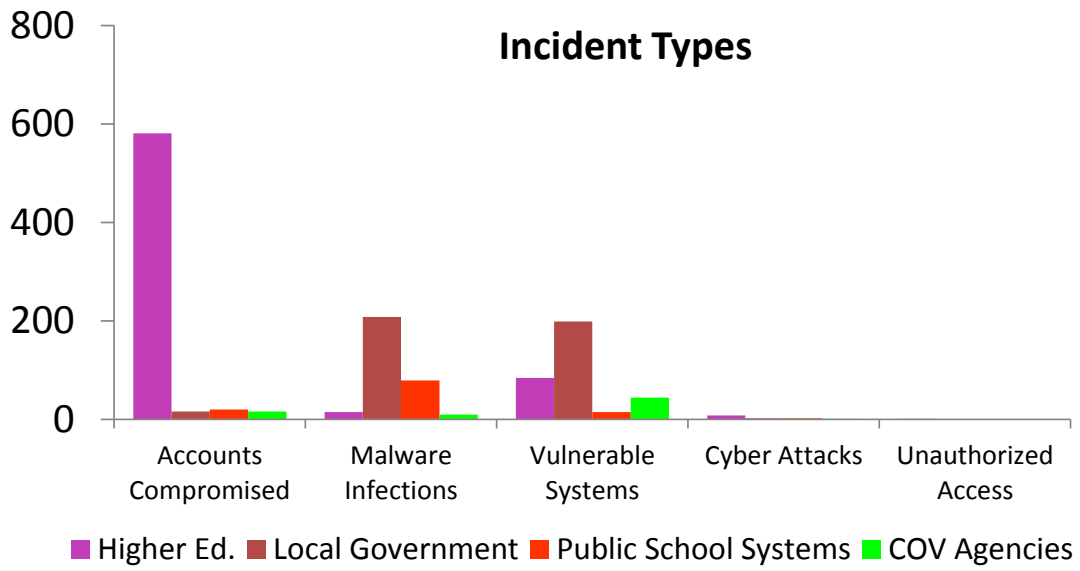


Of the vulnerabilities that were reported, there was an increase in critical exploits, such as zero day exploits. In 2013, there were 66 critical exploits reported. In 2014, this number rose to 165. This is a 150 percent increase in critical exploits.



The information received from Commonwealth partners includes data involving state and local governments, higher education and public schools systems. The majority of the data is reported by the Multi-State Information Sharing and Analysis Center (MS-ISAC) as potential events that they have monitored on the Internet. CSRM disseminates these alerts to the affected entities and tracks these alerts as investigations, since the results of the alert are unknown. In 2014, the Commonwealth completed 231 investigations for the alerts that were received. These alerts were recorded using the similar categories as an incident. The following charts shows the types and amounts of alerts that were received.





An additional service provided by the Commonwealth's cybersecurity incident response program is distribution of cyberintelligence information to both agencies and law enforcement within the Commonwealth. Although a formal intelligence program is not funded, CSRM provides this information and develops relationships with state, federal and local partners. Some of the more notable relationships involve the Virginia Fusion Center, VSP, MS-ISAC, the FBI, the United States Computer Emergency Response Team, and the 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 34 state agencies, 79 localities, 19 colleges and universities, and 34 public school systems to provide notifications of website defacements, compromised accounts, reported vulnerabilities, reported cyberattacks and malware infections.

Formal Cyber Intelligence Program in VITA Is Recommended

Due to the significant increase in cybersecurity incidents, we recommend the Commonwealth fund a formal cyberintelligence program in VITA. This program would provide analysis on threats and attempted attacks that are impacting the Commonwealth. A properly funded cyberintelligence 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 cyberattack attempts. The second benefit is 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. A formal cyber intelligence program would help CSRM understand who is targeting the Commonwealth and why, so better security controls could be implemented.

Commonwealth Information Security Governance

The Commonwealth's information security governance program consists of statutorily-required identification of non-compliant agencies, which is based on formal security policies and standards. These efforts are supported by Commonwealth Information Security Council and the Commonwealth's Information Security Officers Advisory Group (ISOAG).

Statute Requires CIO to Identify Noncompliant Agencies

As directed by §2.2-2009 (C) of the *Code of Virginia,* the CIO is required to identify those agencies who have not implemented acceptable policies, procedures and standards to control unauthorized uses, intrusions or other security threats.

Identification of noncompliant agencies is done through the evaluation of agency audit, risk, and operations programs. The evaluation criteria for each program include:

Information Security Audit Program

- 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

Information Security Risk Program

- Submitted a risk assessment of sensitive IT systems, not less than once every three years
- Submitted agency business impact analysis
- Threat metrics analysis

Information Security Operations Program

- Compliance with current Commonwealth security standards
- Threat and attack analysis

The primary objectives for the Commonwealth's cybersecurity strategy are:

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

Information Security Policies, Standards and Guidelines

The Commonwealth's IT security governance program is formally documented in one policy and five standards designed to assist agencies in building and documenting their individual security programs. The policy sets the Commonwealth's overall direction and establishes a framework that agency heads must follow in implementing IT security programs.

Templates are also available to help agencies develop their own policies. The five standards provide a greater depth of information on the requirements and address the topics of: security controls; security audits; removal of Commonwealth data from surplus computer hard drives and electronic media; use of non-Commonwealth devices for telework; and IT

risk management. An exception process is available if an agency must conduct business in a manner that does not comply with the requirements.

In 2014, CSRM reviewed and adopted changes from NIST 800-53 revision 4 to produce the latest version of our security standard, SEC501-09. The update includes enhancements to controls for insider threats, software application security (including Web applications, social networking, mobile devices, cloud computing, cross domain solutions, advanced persistent threats, industrial/process control systems, and some administrative changes. The new document is more refined, raises the bar for security, and takes into account feedback from ISOs, auditors and others.

The small agency ISO program assisted eight agencies in 2014 with their IT security programs. The areas of assistance for the designated agencies focused on:

- Obtaining ISO certifications for six agencies;
- Providing IT security training information for two agencies;
- Providing documentation for the business impact analysis, formulating the risk assessment, and preparing the IT security audit plan for seven agencies;
- Providing documentation for the risk assessment plan at eight agencies; and
- Assisting with preparation of a business impact analysis at two agencies.

During 2014, CSRM observed that a high risk issue for small agencies was the ability to conduct IT security audits for their sensitive systems. Accordingly, CSRM's small agency ISO program began obtaining information on the implementation of an IT security audit services program to assist small agencies with obtaining IT security audit services. We initially contacted 18 agencies to provide this assistance, and to date the program has assisted two agencies. Several agencies are waiting until after July 2015 to assess their available funding for obtaining IT security audit services.

Commonwealth Information Security Council

The Commonwealth Information Security (IS) 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. The IS Council's purpose is to provide input into the direction of the Commonwealth-wide information security program and to raise awareness of information security topics within the Commonwealth. The IS Council meets monthly to provide direction for the Commonwealth's information security program, and formed committees to address the following five initiatives for 2014:

- The Second Annual Commonwealth of Virginia Information Security Conference
- Information security as a percentage and scope of the IT budget
- IT security standards and policies
- ISO communication and knowledge sharing website
- Assessment of IPV6

Commonwealth Information Security Officer Advisory Group

ISOAG is a dynamic group open to all government personnel. The focus is 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's information security program. Members are also frequently notified of cybersecurity training opportunities in the region. In 2014, ISOAG monthly meeting

keynote speakers included representatives from UVA, VDOT, VDEM, VCU, and various private sector organizations with expertise in information security.

ISOAG meetings averaged 140 attendees per meeting, with many members electing to use our teleconferencing option. Quality keynote speakers and a desire within the Commonwealth's IT security community to maintain current knowledge and understanding of threats and trends have contributed to the increase in average attendance from the previous average of 134.

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 (CPE), a requirement necessary for security professionals to maintain their security certifications and memberships in global security organizations. There is no cost to the attendees.

Given the positive feedback received from attendees, CSRM will continue posting the meeting presentations on the VITA website. We will also continue using webinars to allow attendees to participate remotely.

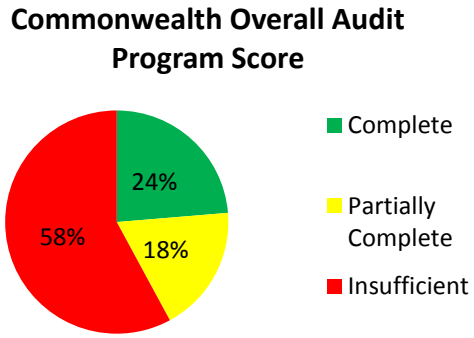
Commonwealth Security Compliance Metrics

No Noticeable Improvement to Information Security Audit Program in 2014

The Commonwealth's IT security and IT security audit standards require agencies to develop and maintain an agency IT security audit program. Agencies are required to appoint a qualified ISO, 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 2014, 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 so they can make risk-based decisions on the allocation of resources within their information security program.

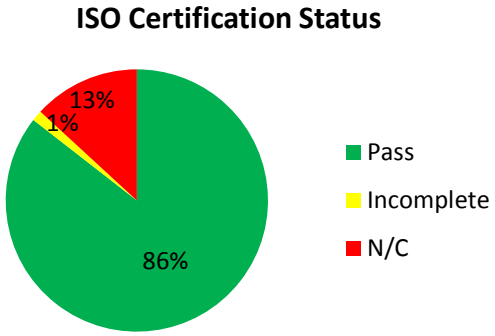
CSRM continues to work toward improving the audit program within the Commonwealth; however, the resources necessary to complete the audits still are not allocated at state agencies. In an attempt to address this issue, CSRM has begun identifying agencies that have inadequate information security audit programs and evaluating whether to prohibit new major technology investments. The desired outcome is that an agency should first address existing information security issues and risks before introducing new technology. CSRM is exploring other methods to tie completion of their programs to information technology funding as well. Unless the security audit program improves, CSRM is limited in identifying areas of weakness within agency environments.



Commonwealth Overall Audit Program Score decreased 7 percent

A certified ISO is the foundation for any successful security audit program. There is a direct correlation between the performance of the information security program and whether the ISO is certified. Given that 65 of 76 ISOs are certified, Virginia is on the right track. Of the 65 ISOs that were certified, 58 (or 89 percent) had audit plans for their agency. In contrast, only half of those ISOs who have not complied with their certification requirements completed an agency audit plan.

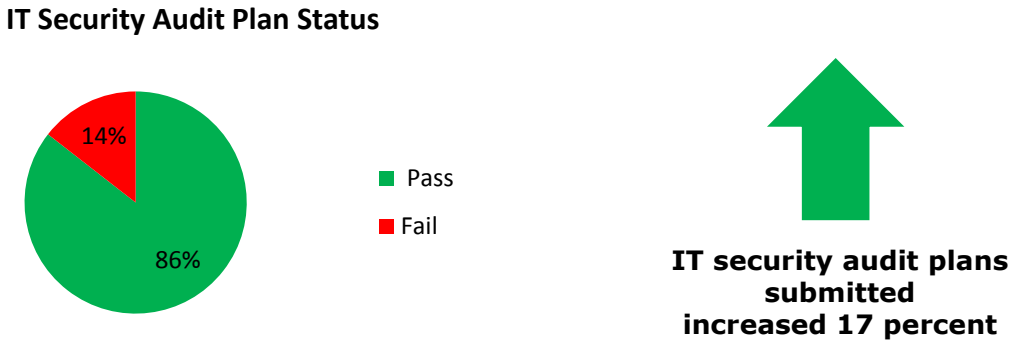
The divergence creates a major obstacle, because a completed and current audit plan is the basis for validating an agency's sensitive system list. Without documented awareness of their environment, an ISO is not able to protect its agency and VITA is not able to accurately define the risk for the agency.



Passing ISO Certifications increased 27 percent

Most agencies have submitted a current information security audit plan for sensitive systems. A security audit is an independent review to assess whether the controls implemented on a system can safeguard effectively the information stored and/or processed by the system. The Commonwealth uses security audits to determine if the proper controls exist and to evaluate them according to the requirements of the Commonwealth Information Security Standard, federal laws, state laws and regulations. Agency heads must take action to have each sensitive system audited every three years. IT security audit plans also provide CSRM with a definitive list of sensitive systems and help the agency schedule the necessary IT security audits for sensitive systems that are identified by the risk management process. Each agency head is required to submit the agency IT security audit plan to the CISO annually.

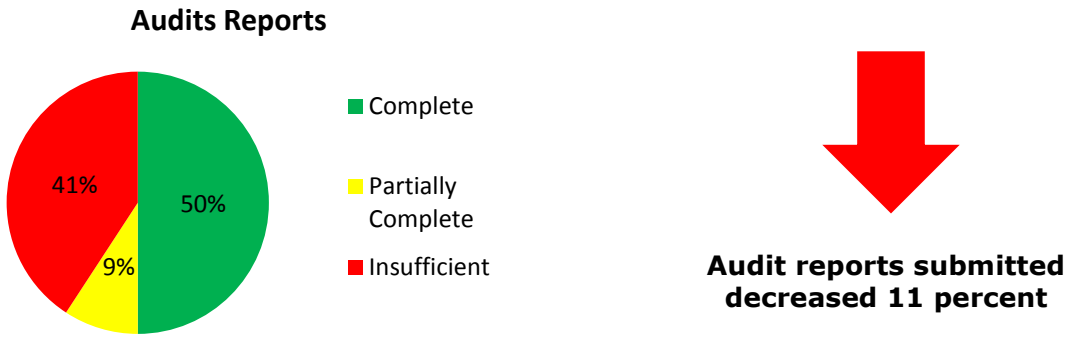
Of the 76 agencies, 65 (86 percent) have submitted a current information security audit plan, and 11 (14 percent) have an expired audit plan.



Half of agencies submitted audit reports for completed 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 76 agencies, 42 agencies had sensitive system IT security audits scheduled for 2014. Thirty-eight (50 percent) have submitted all IT security audit reports that are due; seven (9 percent) have submitted some of the IT security audit reports; and 31 (41 percent) have not submitted any of the IT security audit reports.

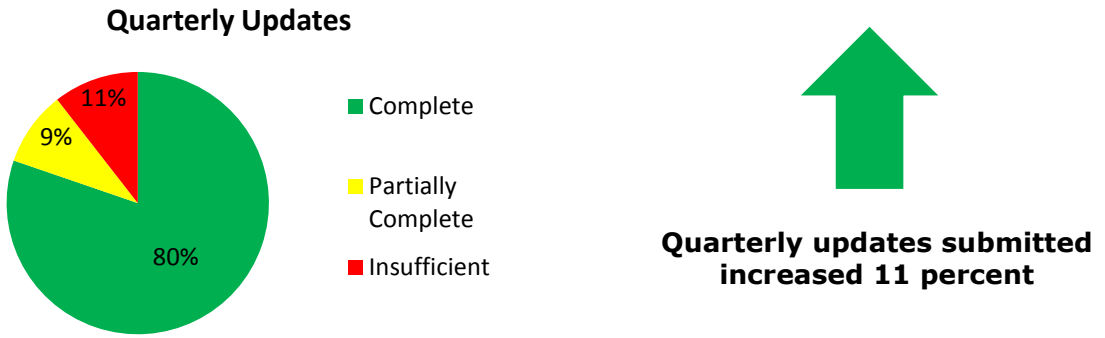
It is important to note that 13 agencies are marked as red or "insufficient" because they did not provide an IT security audit plan. An additional 21 agencies had no IT security audits due for 2014; those agencies are marked as "Complete" in the following pie chart.



Most agencies submitted 2014 quarterly updates for open corrective action plans. In order to track the progress of remedial activities needed to address submitted corrective action plans, agencies are required to provide quarterly updates to the CISO for corrective action plans with open findings. 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.

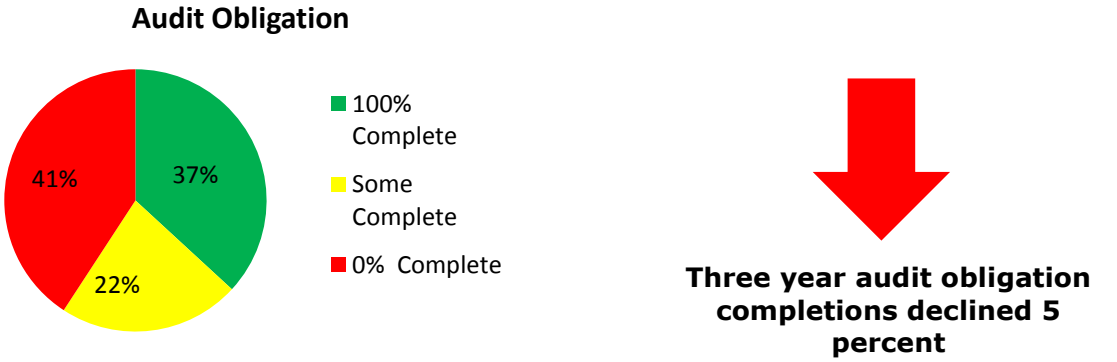
Of the 76 agencies, 30 agencies had quarterly updates due for open corrective action plans in 2014. Of those 30 agencies, 15 (50 percent) have submitted all updates; seven agencies (23 percent) have submitted some of the updates; and 8 agencies (27 percent) have not submitted any updates. The numbers in the chart below appear more optimistic because

they include 46 agencies that were not required to submit quarterly updates and are thus marked as "complete." However, many of these agencies simply did not perform their required audits and thus had no findings or subsequent quarterly updates to report. For agencies tracking findings through completion, an average of 449 days was required to close a finding. On average, findings (whether open or closed within 2014) were open for 392 days.



Less than half of agencies completed required audits. As discussed previously, agency heads must audit each sensitive system 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 76 agencies, 28 (37 percent) have completely fulfilled the obligation to have every sensitive system audited at least once every three years, and 17 (22 percent) have partially fulfilled their audit obligation. At the other end of the spectrum, 31 agencies (41 percent) have not performed any audits or have not submitted evidence to the CISO of an audit for their systems in the last three years.



Security Audit Findings

Almost 1/3 of all security audit findings were related to access control. Access control was the number one security control family identified by auditors, with AC-02 Account Management making up 17 percent of security audit findings. These findings were typically associated with agency-specific applications, and indicate the need for an identity access management standard. CSRM is currently working on an identity access management standard with a target release in 2015.

Access control risk was also found to be widespread, with 69 percent of all agencies that submitted security audits reporting at least one access control-related finding.

Risk assessments had the second highest number of findings, comprising 10 percent of all findings. Information gathered by the CSRM risk team indicates more than half of all agencies do not complete regular risk assessments. However the findings could be higher, because agencies have not been performing the required audits and the risk assessment issues may have gone under-reported. CSRM is working with agencies to identify what can be done to assist them in completing their risk assessments. Initial feedback from agencies indicates that completion is hindered by a lack of available resources allocated to support the information security program.

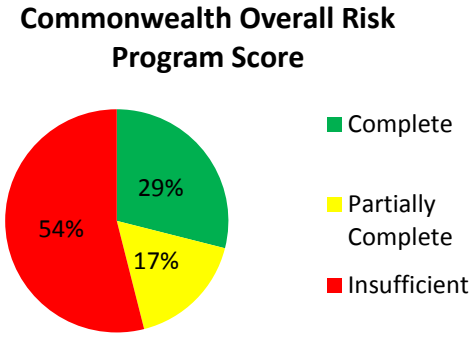
Commonwealth IT Risk Management Program

Commonwealth agencies made improvements in 2014 in the quality of their business impact analyses, risk assessments, and intrusion detection reporting. While the risk management posture has improved since 2012, progress is still needed in the planning and performance of sensitive IT system risk assessments. CSRM anticipates continued improvement in the risk management program as processes mature.

CSRM released a risk management standard in February 2014 incorporating the NIST Cybersecurity framework. 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 understand the risks that they are subject to; and
- Set a risk threshold for the Commonwealth as a whole.

In order to support the risk management framework, CSRM collected sets of data from agencies existing business impact analyses, risk assessments, and data on vulnerabilities and threats. These data are used to develop the Commonwealth's overall risk program score, which indicates that more than half of the agencies have an insufficient risk mitigation program.



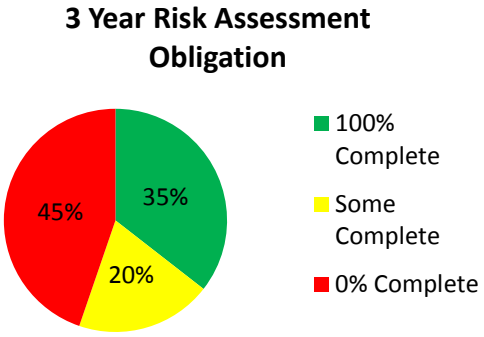
Most agencies submitted compliant business impact analyses. A BIA delineates the steps necessary for agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions. Included within the BIA are data classification and data sensitivity identification activities. The summation of these requirements can provide the input to document a sensitive systems inventory. Of the 76

agencies, 58 (76 percent) submitted BIA documentation. Of the 58 BIAs submitted, 93 percent were deemed to meet all the necessary criteria:

- All business functions that rely on IT are listed;
- All IT systems are aligned with the business functions they support;
- Mission essential functions were identified;
- Recovery time objectives (RTO) were identified;
- Recover point objectives (RPO) were identified;
- Functions that process sensitive data were identified; and
- Business functions are rated for impact to life, safety, finance, legal, regulation/compliance, customer service, reputation and citizen privacy.

Complete BIA submissions decreased 2 percent

Most agencies submitted required risk assessments. A risk assessment is the process of identifying vulnerabilities, threats, likelihood of occurrence and potential loss or impact. Of the 76 agencies, 27 (35 percent) submitted all of the required risk assessment documents. Of the 787 sensitive systems identified, 342 had risk assessments performed.



3 Year Risk Assessment Obligation completions increased 3 percent

Of the agencies reporting risk findings, 82 percent had findings in at least one of these top three control families. This is in strong correlation towhat we found for our IT security audit findings:

- Configuration management
- Access control
- Contingency planning

CSRM will further investigate these findings to see if there is a common cause and possible enterprise resolution.

Few agencies reported performing all required vulnerability scans. Vulnerability scanning is an automated process to determine whether computer systems have vulnerabilities that may be exploitable, putting the system and data at risk. Vulnerability scanning must be performed against multiple layers of IT systems, such as the operating system layer and the application layer, to ensure that both the underlying IT system and the application that sits on top of it are operating at an acceptable level.

In 2014, 71 agencies (93 percent) reported some level of vulnerability scans were performed against their sensitive, public-facing IT systems. However, only 33 agencies (43 percent) performed all of the required application vulnerability scans on their sensitive,

public-facing IT systems. Moreover, five agencies (7 percent) did not submit any of the required vulnerability scans for their systems. Attacks against public-facing Web applications remain a primary method for attackers to gain unauthorized access to sensitive IT systems and data. Forty-three agencies (57 percent) reported they did not perform any Web application vulnerability scans on their sensitive public-facing IT systems and as such, this remains an area of significant concern and area for improvement.

Most agencies submitted required 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. Transformed agencies have their threat metrics reported directly to CSRM on their behalf. Of the 76 agencies, 72 (95 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.

New Cybersecurity Framework Will Strengthen Commonwealth's Security Posture

The cybersecurity framework will strengthen the Commonwealth's ability to fight cybercrime and further enhance Virginia's position as a leader in cybersecurity. The new framework will help to enhance the systematic process for (a) identifying, assessing, prioritizing and communicating cybersecurity risks; (b) efforts to address risks; and (c) steps needed to reduce risks as part of the state's broader priorities.

This is our first year using the cybersecurity framework. The data collected and used in measuring the current profile of the Commonwealth was taken from a variety of different sources. Next year CSRM will work to further refine the data to provide additional insight into the current cybersecurity risk profile.

The 2014 profile is made up of five functions which are used to group agency data within the framework.

Identify: Develop the institutional understanding to manage the information security risks to the organizations IT systems, assets, data and the business functions necessary to accomplish Commonwealth agency missions that they support

Protect: Develop and implement the appropriate safeguards, prioritized through the organization's risk management program to ensure the continued operation of the organization's business functions

Detect: Develop and implement the appropriate activities to identify the occurrence of an information security event

Respond: Develop and implement the appropriate activities, prioritized through the organization's risk management process, to take action regarding a detected information security event

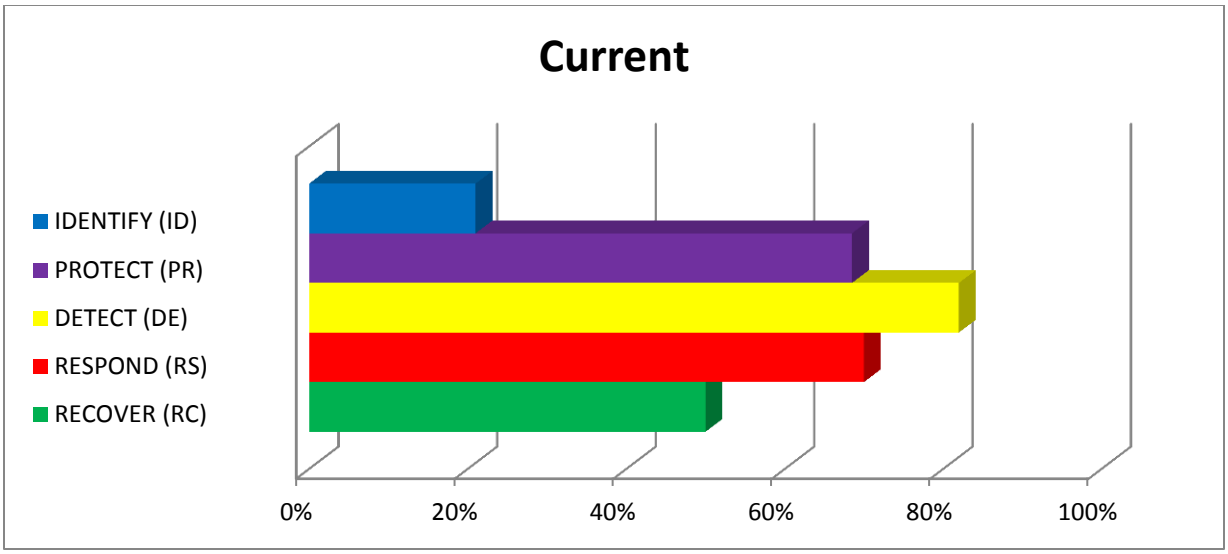
Recover: Develop and implement the appropriate activities, prioritized through the organization's risk management process, to take action regarding a detected information security event

In order to measure the current cybersecurity profile, CSRM used a combination of information security program documentation and the results of security audits and risk

assessments to determine the maturity of each function. CSRM will work to identify the function maturity for each agency over the next year. The following table identifies the data used to measure each function.

Function	Basis for Measurement	Target
IDENTIFY (ID)	Three-Year Risk Assessment Obligation and Three-Year Audit Obligation are used to determine the Identify score.	100% - Indicates an updated sensitive system list with risk assessments and IT security audits performed on all sensitive systems in past three years.
PROTECT (PR)	Percent of ISOs certified and related findings are used for the Protect score.	100% - Indicates all ISOs certified and related findings should take fewer than 180 days to remediate
DETECT (DE)	Quarterly IDS reports, operating system vulnerability scanning, sensitive system scans and Web page scans are factored into the Detect score.	100% - Indicates when all four IDS reports were submitted with all required information and vulnerability scans performed for all necessary systems.
RESPOND (RS)	Average days open for IT Security Audits and Risk Assessment findings were used for the Respond score.	100% - Indicates when an agency responded on average to remediate findings within 180 days, or had no findings.
RECOVER (RC)	Findings associated with Recover were used for the scoring.	100% - Indicates that related findings took fewer than 180 days to remediate

The Commonwealth's current risk posture is calculated based on results against target 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.


Current
IDENTIFY (ID)
PROTECT (PR)
DETECT (DE)
RESPOND (RS)
RECOVER (RC)
0%
20%
40%
60%
80%
100%

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.

Met ISO Certification Requirements

- The Primary ISO is certified
- The Primary ISO met some of the requirements
- The Primary ISO is NOT certified.

2014 Overall Audit Program

- Documents received as scheduled
- Missing CAP(s) or Quarterly update(s)
- Missing Audit plan
- Have not met audit obligation

2014 Overall Risk Profile

- All documentation received as requested information about the agency's vulnerability scans, BIA, RA(s)[1] , and IDS reports
- Partially submitted requirements
- Missing any required documentation as requested information about the agency's vulnerability scans, BIA and RA(s), and IDS reports

Agency Information Security Datapoints – Dashboard

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

COV: Agency Data Points

Agency Name	Secretariat	Acronym	ISO Designated	Overall Audit Program	Overall Risk Profile
Alcoholic Beverage Control	Public Safety	ABC	Yes		
Board of Accountancy	Commerce and Trade	BOA	Yes		
Center for Innovative Technology	Technology	IEIA	Yes		
Commonwealths Attorney's Services Council	Public Safety	CASC	Yes		
Compensation Board	Administration	CB	Yes		
Comprehensive Services for At-Risk Youth and Families	Health and Human Resources	CSA	Yes		
Department for Aging and Rehabilitative Services	Health and Human Resources	DARS	Yes		
Department of Accounts	Finance	DOA	Yes		
Department of Aviation	Transportation	DOAV	Yes		
Dept. of Behavioral Health & Developmental Services	Health and Human Resources	DBHDS	Yes		
Department of Conservation and Recreation	Natural Resources	DCR	Yes		
Department of Corrections	Public Safety	DOC	Yes		
Department of Criminal Justice Services	Public Safety	DCJS	Yes		
Department of Education	Education	DOE	Yes		
Department of Elections	Administration	ELECT	Yes		
Department of Environmental Quality	Natural Resources	DEQ	Yes		
Department of Fire Programs	Public Safety	DFP	Yes		
Department of Forensic Science	Public Safety	DFS	Yes		
Department of Forestry	Agriculture & Forestry	DOF	Yes		
Department of Game and Inland Fisheries	Natural Resources	DGIF	Yes		
Department of General Services	Administration	DGS	Yes		
Department of Health Professions	Health and Human Resources	DHP	Yes		
Department of Historic Resources	Natural Resources	DHR	Yes		
Department of Housing and Community Development	Commerce and Trade	DHCD	Yes		
Department of Human Resource Management	Administration	DHRM	Yes		
Department of Juvenile Justice	Public Safety	DJJ	Yes		

COV: Agency Data Points

Department of Labor and Industry	Commerce and Trade	DOLI	Yes		
Department of Medical Assistance Services	Health and Human Resources	DMAS	Yes		
Department of Military Affairs	Public Safety	DMA	Yes		
Department of Mines, Minerals and Energy	Commerce and Trade	DMME	Yes		
Department of Motor Vehicles	Transportation	DMV	Yes		
Department of Planning and Budget	Finance	DPB	Yes		
Department of Professional and Occupational Regulation	Commerce and Trade	DPOR	Yes		
Department of Rail and Public Transportation	Transportation	DRPT	Yes		
Department of Small Business and Supplier Diversity	Commerce and Trade	SBSD	Yes		
Department of Social Services	Health and Human Resources	DSS	Yes		
Department of Taxation	Finance	TAX	Yes		
Department of Treasury	Finance	TD	Yes		
Department of Veterans Services	Public Safety	DVS	Yes		
Frontier Culture Museum of Virginia	Education	FCMV	Yes		
Gunston Hall	Education	GH	Yes		
Indigent Defense Commission	Independent	IDC	Yes		
Jamestown-Yorktown Foundation	Education	JYF	Yes		
Library of Virginia	Education	LVA	Yes		
Marine Resources Commission	Natural Resources	MRC	Yes		
Motor Vehicle Dealers Board	Transportation	MVDB	Yes		
Norfolk State University	Education	NSU	Yes		
Office of Attorney General	Executive	OAG	Yes		
Office of State Inspector General	Executive	OSIG	Yes		
Office of the Governor	Executive	GOV	Yes		
Richard Bland College	Education	RBC	Yes		
Science Museum of Virginia	Education	SMV	Yes		
Southern Virginia Higher Education Center	Education	SVHEC	Yes		
State Corporation Commission	Independent	SCC	Yes		
State Council of Higher Education for Virginia	Education	SCHEV	Yes		
State Lottery Department	Independent	SLD	Yes		

COV: Agency Data Points

Tobacco Indemnification Commission	Commerce and Trade	TIC	Yes		
Virginia College Savings Plan	Independent	VCSP	Yes		
Virginia Commission for the Arts	Education	VCA	Yes		
Virginia Dept. of Agriculture and Consumer Services	Agriculture & Forestry	VDACS	Yes		
Virginia Department of Emergency Management	Public Safety	VDEM	Yes		
Virginia Department of Health	Health and Human Resources	VDH	Yes		
Virginia Department of Transportation	Transportation	VDOT	Yes		
Virginia Economic Development Partnership	Commerce and Trade	VEDP	Yes		
Virginia Employment Commission	Commerce and Trade	VEC	Yes		
Virginia Foundation for Healthy Youth	Health and Human Resources	VFHY	Yes		
Virginia Information Technologies Agency	Technology	VITA	Yes		
Virginia Museum of Fine Arts	Education	VMFA	Yes		
Virginia Museum of Natural History	Natural Resources	VMNH	Yes		
Virginia Racing Commission	Commerce and Trade	VRC	Yes		
Virginia Resources Authority	Commerce and Trade	VRA	Yes		
Virginia Retirement System	Independent	VRS	Yes		
Virginia School for the Deaf and Blind	Education	VSDB	Yes		
Virginia State Police	Public Safety	VSP	Yes		
Virginia State University	Education	VSU	Yes		
Virginia Workers Compensation Commission	Independent	VWC	Yes		

Appendix II - Agency Information Security Datapoints - Dashboard

Agency Information Security Datapoints Dashboard - Legend

Attended IS Orientation, KC Training and ISOAG Meetings

Pass - The primary ISO is certified

Incomplete - The ISO met all other requirements but did not attend the mandatory ISOAG meeting

N/C - The primary ISO is NOT certified

2014 Audit Plan Status

Pass - Documents received as scheduled

N/C - Missing audit plan

COV: Agency Data Points

2014 Business Impact Analysis Status

Pass - All documentation received as requested

Incomplete - Documentation received, but incomplete

N/C - Documentation was not submitted

Percentage of Audits 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

N/C - The agency head has not submitted a security audit plan

Audit Reports Received and Quarterly Updates Received

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

N/A - Not applicable as the agency had no quarterly updates due or the agency head has not submitted a security audit plan

Percentage of 3 Year Audit Obligation Completed

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

N/A - Not applicable as the agency had no audits due

N/C - The agency head has not submitted a security audit plan

Percentage of 3 Year Risk Assessment Obligation Completed

X% - The percentage of risk assessment work completed as measured against the agency's sensitive systems over the past three years

N/A - Not applicable as the agency had no risk assessments due

N/C - The agency head has not submitted an audit plan

Agency Secretariat	Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
Public Safety	ABC	Pass	Pass	100%	100%	73%	Pass	45%	Pass	Pass	Pass
Commerce and Trade	BOA	Pass	Pass	N/A	N/A	100%	Pass	100%	Pass	Pass	Pass
Technology	IEIA	Pass	Pass	0%	N/A	0%	Pass	100%	Pass	Pass	Pass
Public Safety	CASC	N/C	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Administration	CB	Pass	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Health and Human Resources	CSA	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Health and Human Resources	DARS	Pass	Pass	100%	100%	100%	N/C	N/C	N/C	Pass	Incomplete
Finance	DOA	Pass	Pass	0%	N/A	53%	Pass	0%	Pass	Pass	Pass
Transportation	DOAV	Pass	Pass	N/A	100%	100%	Pass	100%	Pass	Pass	Pass

COV: Agency Data Points

Health and Human Resources	DBHDS	Pass	N/C	N/C	N/A	N/C	Pass	100%	Pass	Pass	Incomplete
Natural Resources	DCR	Pass	Pass	100%	0%	100%	N/C	N/C	Pass	Pass	Incomplete
Public Safety	DOC	Pass	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Public Safety	DCJS	N/C	PASS	N/C	N/A	N/C	N/C	N/C	Pass	Pass	Incomplete
Education	DOE	Pass	N/C	N/C	N/A	N/C	N/C	N/C	Pass	Pass	Pass
Administration	ELECT	Pass	Pass	0%	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Natural Resources	DEQ	Pass	N/C	N/C	0%	N/C	N/C	N/C	Pass	Pass	Incomplete
Public Safety	DFP	Pass	Pass	N/A	N/A	0%	N/C	N/C	Pass	Pass	Incomplete
Public Safety	DFS	Pass	Pass	0%	N/A	25%	Pass	100%	Pass	Pass	Pass
Agriculture & Forestry	DOF	Pass	Pass	100%	67%	24%	Pass	100%	Pass	Pass	Pass
Natural Resources	DGIF	Pass	Pass	0%	N/A	0%	N/C	N/C	N/C	Pass	Incomplete
Administration	DGS	Incomplete	Pass	100%	0%	100%	N/C	N/C	N/C	Pass	Incomplete
Health and Human Resources	DHP	Pass	Pass	100%	N/A	50%	Pass	100%	Pass	Pass	Pass
Natural Resources	DHR	Pass	Pass	0%	33%	N/A	Pass	N/A	Pass	Pass	Pass
Commerce and Trade	DHCD	Pass	Pass	0%	0%	0%	N/C	N/C	N/C	Pass	Incomplete
Administration	DHRM	Pass	Pass	0%	N/A	0%	N/C	N/C	Incomplete	Pass	Incomplete
Public Safety	DJJ	Pass	Pass	0%	100%	100%	Pass	100%	Pass	Pass	Incomplete
Commerce and Trade	DOLI	Pass	N/C	N/C	N/A	N/C	Pass	57%	Pass	Pass	Pass
Health and Human Resources	DMAS	Pass	Pass	20%	100%	84%	N/C	N/C	N/C	Pass	Pass
Public Safety	DMA	N/C	PASS	N/C	N/A	N/C	Pass	N/A	Pass	Pass	Incomplete
Commerce and Trade	DMME	Pass	Pass	0%	0%	0%	N/C	N/C	Pass	Pass	Incomplete
Transportation	DMV	Pass	Pass	100%	43%	16%	Pass	66%	Pass	Pass	Incomplete
Finance	DPB	Pass	Pass	N/A	N/A	0%	Pass	0%	Pass	Pass	Incomplete
Commerce and Trade	DPOR	Pass	Pass	N/A	100%	100%	Pass	100%	Pass	Pass	Incomplete
Transportation	DRPT	Pass	Pass	N/A	N/A	0%	N/C	N/C	Pass	Pass	Incomplete
Commerce and Trade	SBSD	N/C	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Health and Human Resources	DSS	N/C	Pass	0%	0%	5%	N/C	N/C	Pass	Pass	Incomplete
Finance	TAX	Pass	Pass	93%	100%	93%	Pass	30%	N/C	Pass	Incomplete
Finance	TD	Pass	PASS	40%	N/A	40%	Pass	100%	Pass	Pass	Pass
Public Safety	DVS	Pass	Pass	N/A	N/A	100%	Pass	100%	Pass	Pass	Pass
Education	FCMV	Pass	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Education	GH	Pass	Pass	N/A	N/A	N/A	Pass	100%	Pass	Pass	Incomplete

COV: Agency Data Points

Independent	IDC	Pass	Pass	0%	0%	N/A	Pass	100%	Pass	Pass	Fail
Education	JYF	Pass	Pass	N/A	N/A	17%	Pass	100%	Pass	Pass	Pass
Education	LVA	Pass	Pass	100%	N/A	100%	Pass	67%	Pass	Pass	Pass
Natural Resources	MRC	Pass	Pass	0%	N/A	100%	Pass	100%	Pass	Pass	Pass
Transportation	MVDB	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Education	NSU	Pass	Pass	50%	N/A	47%	N/C	N/C	N/C	Pass	Fail
Executive	OAG	N/C	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Executive	OSIG	Pass	Pass	N/A	N/A	N/A	Pass	N/A	Pass	Pass	Pass
Executive	GOV	Pass	Pass	0%	N/A	0%	Pass	100%	Pass	Pass	Pass
Education	RBC	Pass	Pass	100%	N/A	100%	Pass	40%	Pass	Pass	Incomplete
Education	SMV	Pass	Pass	N/A	N/A	N/A	Pass	100%	Pass	Pass	Pass
Education	SVHEC	Pass	Pass	N/A	N/A	N/A	Pass	N/A	N/C	Fail	Pass
Independent	SCC	Pass	Pass	33%	110%	100%	N/C	N/C	Pass	Pass	Pass
Education	SCHEV	Pass	Pass	100%	N/A	25%	N/C	N/C	N/C	Pass	Incomplete
Independent	SLD	Pass	Pass	40%	25%	67%	Pass	0%	Incomplete	Fail	Fail
Commerce and Trade	TIC	Pass	Pass	0%	N/A	0%	N/C	N/C	Pass	Pass	Incomplete
Independent	VCSP	Pass	Pass	100%	N/A	100%	Pass	100%	Pass	Pass	Pass
Education	VCA	N/C	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Agriculture & Forestry	VDACS	Pass	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Incomplete
Public Safety	VDEM	Pass	Pass	N/A	N/A	0%	N/C	N/C	Pass	Pass	Fail
Health and Human Resources	VDH	Pass	Pass	100%	100%	86%	N/C	N/C	Pass	Pass	Incomplete
Transportation	VDOT	N/C	Pass	100%	100%	100%	Pass	100%	Incomplete	Pass	Pass
Commerce and Trade	VEDP	Pass	Pass	N/A	N/A	0%	Pass	N/A	Pass	Fail	Pass
Commerce and Trade	VEC	Pass	Pass	0%	100%	61%	N/C	N/C	N/C	Fail	Fail
Health and Human Resources	VFHY	N/C	Pass	N/A	N/A	N/A	Pass	N/A	N/C	Pass	Incomplete
Technology	VITA	Pass	Pass	100%	75%	100%	Pass	75%	Pass	Pass	Pass
Education	VMFA	Pass	Pass	N/A	0%	0%	N/C	N/C	Incomplete	Pass	Pass
Natural Resources	VMNH	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Commerce and Trade	VRC	Pass	Pass	N/A	N/A	N/A	Pass	N/A	Pass	Pass	Pass
Commerce and Trade	VRA	N/C	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Independent	VRS	Pass	Pass	0%	73%	100%	N/C	N/C	Pass	Pass	Pass
Education	VSDB	Pass	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete

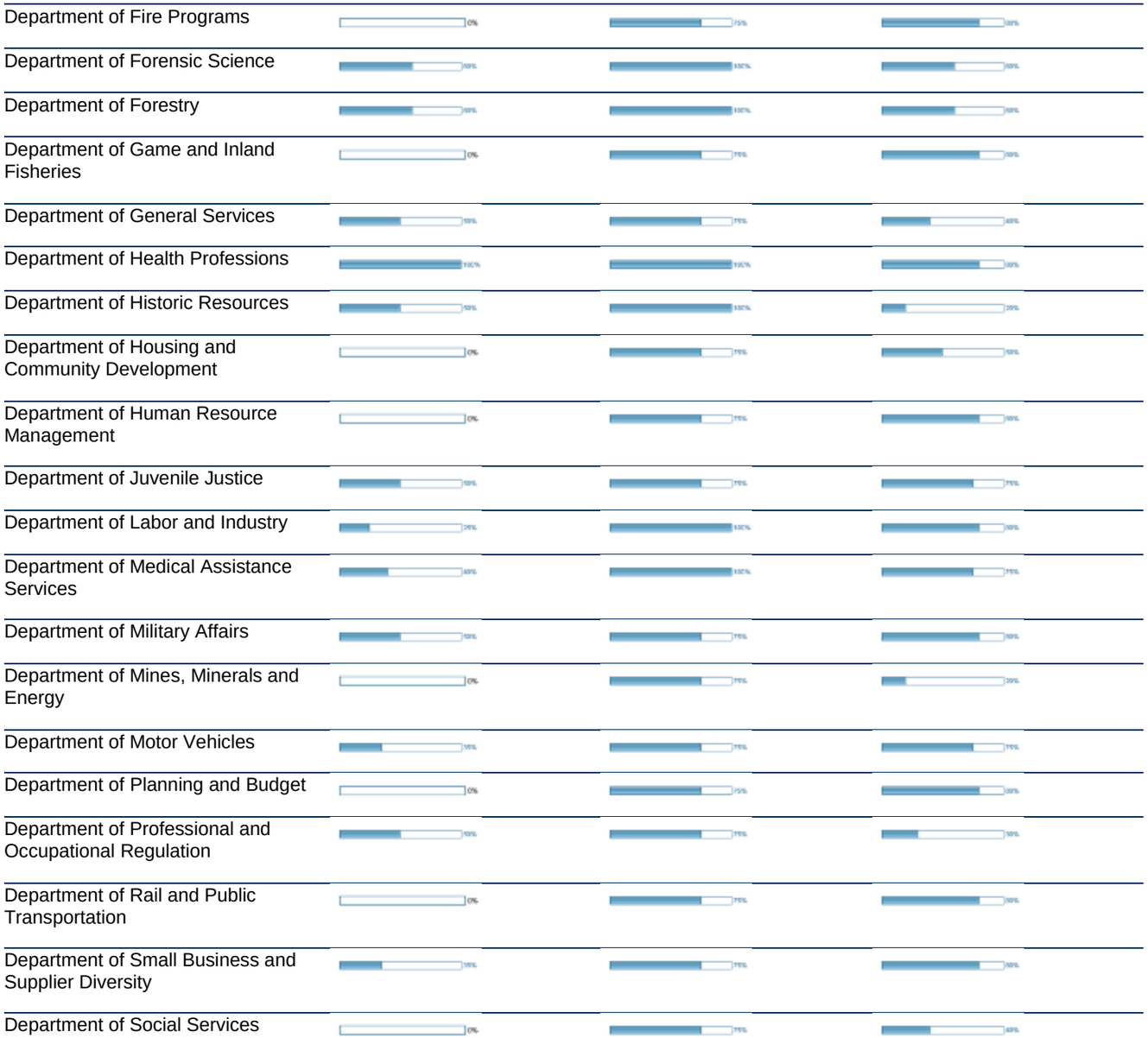
COV: Agency Data Points

Public Safety	VSP	Pass	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Education	VSU	Pass	Pass	80%	100%	76%	Pass	0%	Pass	Pass	Pass
Independent	VWC	Pass	Pass	0%	100%	100%	Pass	75%	Pass	Pass	Pass

Risk Framework

Agency Name	Identify	Detect	Respond
Alcoholic Beverage Control			
Board of Accountancy			
Center for Innovative Technologies			
Commonwealths Attorney's Services Council			
Compensation Board			
Comprehensive Services for At-Risk Youth and Families			
Department for Aging and Rehabilitative Services			
Department of Accounts			
Department of Aviation			
Department of Behavioral Health and Development Services			
Department of Conservation and Recreation			
Department of Corrections			
Department of Criminal Justice Services			
Department of Education			
Department of Elections			
Department of Environmental Quality			

COV: Agency Data Points



COV: Agency Data Points

Department of Taxation			
Department of Treasury			
Department of Veterans Services			
Frontier Culture Museum of Virginia			
Gunston Hall			
Indigent Defense Commission			
Jamestown-Yorktown Foundation			
Library of Virginia			
Marine Resources Commission			
Motor Vehicle Dealers Board			
Norfolk State University			
Office of Attorney General			
Office of State Inspector General			
Office of the Governor			
Richard Bland College			
Science Museum of Virginia			
Southern Virginia Higher Education Center			
State Corporation Commission			
State Council of Higher Education for Virginia			
State Lottery Department			
Tobacco Indemnification Commission			
Virginia College Savings Plan			
Virginia Commission for the Arts			

COV: Agency Data Points

Virginia Department of Agriculture and Consumer Services			
Virginia Department of Emergency Management			
Virginia Department of Health			
Virginia Department of Transportation			
Virginia Economic Development Partnership			
Virginia Employment Commission			
Virginia Foundation for Healthy Youth			
Virginia Information Technologies Agency			
Virginia Museum of Fine Arts			
Virginia Museum of Natural History			
Virginia Racing Commission			
Virginia Resources Authority			
Virginia Retirement System			
Virginia School for the Deaf and Blind			
Virginia State Police			
Virginia State University			
Virginia Workers Compensation Commission			