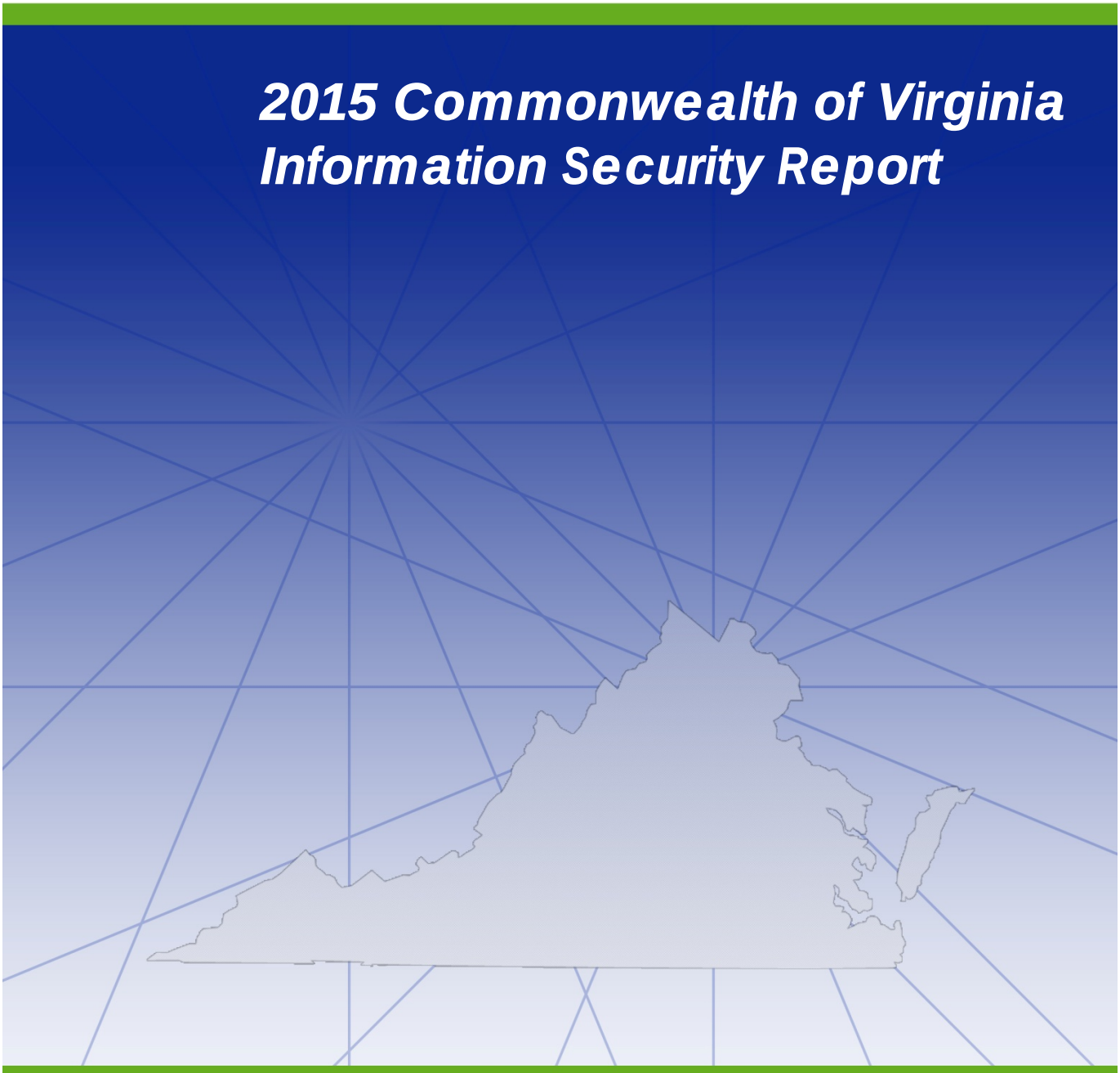
Virginia Information Technologies Agency

2015 Commonwealth of Virginia Information Security Report



www.vita.virginia.gov

Prepared and Published by:

Virginia Information Technologies Agency

VITA - Powering the commowealth's digital government

Comments on the
2015 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

2015 Information Security Report

Executive Summary

This 2015 Commonwealth of Virginia (COV) Information Security Report is the eighth annual report by the chief information officer (CIO) of the commonwealth to the governor and the General Assembly. As directed by §2.2-2009 (B.1) of the *Code of Virginia,* the CIO is required to identify annually 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 (B.1), the scope of this report is limited to the six independent and 71 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 77 agencies assessed in this report and their specific security information concerns can be found in the Appendix Data Points - Dashboard.

VITA's cyber-related risk management activities increased with the governor's issuance of Executive Directive 6. The directive required VITA to provide an updated inventory of all data and computer systems. This inventory included the determination of sensitivity and criticality of systems and data, risk prioritization and scope of systems and data, and development of a risk-based approach to enhance the protection of systems and data. As a result, CSRM surveyed the agencies to determine the nature of the applications and data maintained by the agency. For systems that were determined to be sensitive, CSRM obtained additional information security and operations management information to evaluate the controls and risks to commonwealth data. IT systems were classified as sensitive based on the degree to which a compromise of the confidentiality, integrity, and/or availability the systems' data could have a material adverse effect on the commonwealth's interests, the conduct of agency programs, or privacy of information. Confidentiality denoted protection from unauthorized disclosure. Integrity entailed protection from intentional or accidental unauthorized modification. Availability represented accessibility to authorized users when needed without interference or obstruction. Agencies classify each IT system by sensitivity according to the most sensitive data that the IT system stores, processes, or transmits. Based on the survey results, CSRM determined that the number of sensitive systems in the commonwealth increased from 740 systems to approximately 1,700 sensitive systems. As VITA begins to provide agency information security officer (ISO) services, we anticipate that resources will be allocated appropriately to evaluate these systems and assess their information security risk.

The governor and the General Assembly enacted legislation to establish an information technology security service center operated by VITA. As directed by the 2016 Appropriation Act, the service center will support the effectiveness of agencies' information security programs by providing security services, including vulnerability scans, information technology security audits, risk management and other IT security services to executive branch agencies. The budget also gives VITA responsibility to conduct vulnerability scans of all public-facing websites and systems that are operated by state agencies. VITA anticipates implementing these services in the summer of 2016.

Information security program compliance was evaluated by CSRM when reviewing requests for information technology investments and off-premise hosting. Agencies that had inadequate information security audit programs were discouraged from beginning new, major technology investments until they addressed their existing information security issues and risks. This effort was designed to help ensure that agencies prioritize funding and resources to address existing information security concerns before beginning new projects. As agencies migrate to third party vendors that provide software specific services, the IT security programs at state agencies have become more important. However, most agencies currently aren't equipped with resources or technology to oversee and manage vendors. As a result, CSRM continues to work with agencies to understand their risk posture and determine secure solutions. VITA will be standing up third party hosting services in 2016 to provide an additional service to the commonwealth.

CSRM recommends all agencies address risks associated with an insecure hash algorithm currently used to sign digital certificates. Standard Hash Algorithm 1 (SHA-1) certificates, a commonly used algorithm used to encrypt web connections and verify the validity of websites, poses a significant security risk. Researchers have determined that attackers could exploit the algorithm's vulnerabilities to gain unauthorized access to information and systems on line. Some browsers have already started phasing out trust for the SHA-1 certificates and showing warnings for sites using SHA-1 certificates. The National Institute of Standards and Technology (NIST) has recommended that all federal agencies adopt SHA-256 (SHA-2), a stronger and more robust cryptographic hashing algorithm. CSRM recommends that agencies develop plans to migrate from SHA-1 to SHA-2 to better secure websites, intranet communications and applications in the commonwealth.

Results of "mock" phishing campaign indicated many commonwealth employees are aware of risks, but about 10 percent provided their credentials. To help evaluate security awareness throughout the commonwealth, CSRM conducted this informational exercise by sending 40,896 simulated phishing emails to employees at 91 agencies. Of the emails sent, 21,632 (53 percent) were opened by the recipient. Of those who opened the emails, 5,384 (13 percent of sent emails, and 25 percent of emails opened) clicked on the link inside the email. Another 3,348 users submitted their credentials in response to the phishing emails, representing 8 percent of all of the emails sent and 15 percent of the emails that were opened. This response indicated many employees in the commonwealth were aware of the risks associated with emails from an unknown sender. However, there is still a need to continue to educate employees on the dangers of opening and responding to emails from an unknown sender and raise information security awareness.

Access control continues to be a significant area of weakness for the commonwealth. Access control failures are responsible for most security-related findings, accounting for 26 percent of all security audit findings. In addition, access controls are related to 32 percent of all requests for security exceptions. While CSRM noted that 45 access control findings were remediated in 2015, access control risk is still prevalent in the commonwealth. 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 develop a security standard for identity access management. Furthermore, agencies having difficulty identifying risks or evaluating controls should consider using the VITA service center that will be offered in fiscal year (FY) 2017 that will include IT risk management and IT audit services.

CSRM took steps to respond to the increasing number of vulnerabilities in 2015. The number of vulnerabilities increased by 42 percent over the prior year. This contributed to the 49 percent increase in the number of incidents compared to the prior year. In the first quarter of 2015, the number of incidents increased slightly from the fourth quarter of 2014 due to a continuing phishing campaign against COV users. The campaign continued through February 2015. During the third quarter of 2015, there was a spike in the number of malware-related incidents due to the Adobe Flash zero day vulnerabilities. These vulnerabilities were being exploited before patches were available. Due to the criticality of these patches, CSRM was able to work with our IT sourcing partner to get the security patches tested and deployed to COV devices in a little over two weeks, about half the time it takes for a normal patch cycle. CSRM will continue to work diligently to investigate and respond to incidents.

Overall risk program compliance needs improvement. In 2015, 65 percent of agency risk programs were not compliant with commonwealth risk program requirements. Since risk management is a key aspect of the commonwealth’s information security program, CSRM will continue to work with agencies to promote the completion and submission of business impact analysis (BIA), risk assessments and other risk program components to help ensure agencies have properly identified and planned for the risk in their environments.

Cyberattacks and other incidents at Virginia colleges and universities remain a significant risk to information security in the commonwealth. These institutions are generally exempt from compliance with commonwealth security requirements, and they are attractive targets for malicious third parties due to the type of information they maintain, including personally identifiable information, health information, and intellectual property. According to Multi-State Information Sharing and Analysis Center (MS-ISAC) statistics, higher education leads other public entities with the highest number of security investigations related to potential accounts compromised, malware infections, website defacement and cyberattacks. Higher education also has the highest estimated cost per incident. CSRM recommends that standard governance requirements be established for these entities and that the institutions should be required to report on metrics similar to the ones used in this annual report to monitor progress. In addition, 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.

CSRM promoted information security education and awareness in the commonwealth. CSRM supported monthly Information Security Officers Advisory Group (ISOAG) meetings to provide security training and facilitate knowledge exchange. In 2015, more than 1,700 security professionals attended the ISOAG meetings. In addition, CSRM utilized the ISO Security Council as a resource to assist in the sharing of best practices between agencies and as major contributors to the 2015 COV Information Security Conference in April 2015. The conference, designed for security and other IT professionals, was well attended. The theme of the conference was “Unifying the Business Enterprise.” Subject matter experts addressed a variety of information security topics, including

regulatory compliance, the internet of things, organizational resilience, cybersecurity breaches and big data. The sold-out event was highly successful.

2015 Annual Security Report Detail

The 2015 Annual Security Report for the Commonwealth of Virginia is included below. The report includes an analysis the commonwealth threat management program, commonwealth information security governance and the commonwealth compliance metrics.

Commonwealth Threat Management Program

Threat management 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 within the VITA IT infrastructure program, as well as agencies falling outside the scope of the IT infrastructure program. This information is analyzed to identify threats affecting the commonwealth and identify widespread vulnerabilities and respond appropriately.

Risks associated with insecure encryption algorithms need to be addressed. The SHA-1 certificates pose a security risk as researchers have determined that attackers could exploit its vulnerabilities to gain unauthorized access to information. Some internet browsers have already started phasing out trust for these by showing warnings for sites still using SHA-1 certificates. Most browsers will no longer support these certificates by 2017. NIST has recommended that all federal agencies adopt SHA-256 (SHA-2), a stronger and more robust cryptographic hashing algorithm. CSRM recommends that agencies work with their IT sourcing partner to inventory their SHA-1 certificates, acquire replacement certificates, test the new certificates with their applications and implement new certificates where needed.

VITA is developing cyber incident response (IR) "playbooks" to streamline the response to cyberattacks. With input from agency and cyber security leaders, VITA will establish comprehensive "playbooks" to improve IR response. The "playbooks" will include detailed IR response practices and procedures with the goal of improving consistency and enhancing the overall effectiveness and efficiency of the threat management program.

Higher risks to commonwealth result from IT that is outside of the enterprise framework. Certain areas of the commonwealth's IT environment are not protected by the enterprise security controls provided by VITA's IT 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 security tools for non-transformed agencies and improved IT security governance and reporting for institutions of higher education independent agencies.

Non-transformed agencies remain at significant information security risk. These agencies remain in an insecure state and are at a substantially elevated risk for intrusion, compromise and disruption. The Virginia Department of Emergency Management (VDEM) and Virginia Employment Commission (VEC) are making progress toward transformation. Once fully transformed, these agencies will have additional protections and resources to protect their networks and information.

In contrast, Virginia State Police (VSP) continues to operate outside of the enterprise security infrastructure and is vulnerable to attacks that would otherwise be mitigated by monitoring, intrusion detection, firewalls, encryption, virtual private networks (VPN) and other enterprise tools. Risks are increasing as software expires and new applications are put into production. CSRM recommends that VSP complete the transformation process as soon as possible. If transformation is not completed, it is highly likely to cost the agency a significant amount of additional resources to have equivalent enterprise security controls put in place. Additionally, should VSP attempt to implement the necessary enterprise security controls on their own, the amount of risk incurred warrants that the secretary of public safety accept the risks related to this action.

CSRM and agencies will play a significant role in defining security requirements for IT sourcing effort. In recognition that the comprehensive infrastructure services agreement with Northrop Grumman will expire in 2019, CSRM and agencies have begun IT sourcing planning and analysis. CSRM will be involved in developing the strategy for new solutions and helping ensure that confidentiality, integrity and availability of the commonwealth's information is a key consideration in all the sourcing decisions.

CSRM will facilitate cyber intelligence sharing through the commonwealth's Information Sharing and Analysis Organization (ISAO). An additional service provided by the Commonwealth's Security Incident Response Team (CSIRT) is the distribution of cyber intelligence information to both agencies and law enforcement within the commonwealth. CSIRT 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 Federal Bureau of Investigations (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.

During 2015, the CSIRT has disseminated intelligence information to 29 state agencies, 59 localities, 21 colleges and universities and 44 public school systems regarding website defacements, compromised accounts, malware infections, reported cyberattacks and vulnerable systems. The relationships developed by the CSIRT allow information sharing to occur and have provided CSRM the opportunity to act as a coordinator and provider of input to the ISAO.

CSRM's CSIRT team will develop a relationship with the ISAO to allow the sharing of intelligence information. They will determine the most actionable intelligence derived from our partners and daily business to provide to the ISAO for analysis. CSRM has seen evidence of targeted attacks against the commonwealth. However, up to this point, we have only been able to investigate individual security incidents. Working with the ISAO on the analysis of the intelligence data collected will help CSRM understand who is targeting the commonwealth and why commonwealth information is being attacked, so that additional security controls can be implemented.

Commonwealth Cyber Threat and Attack Analysis

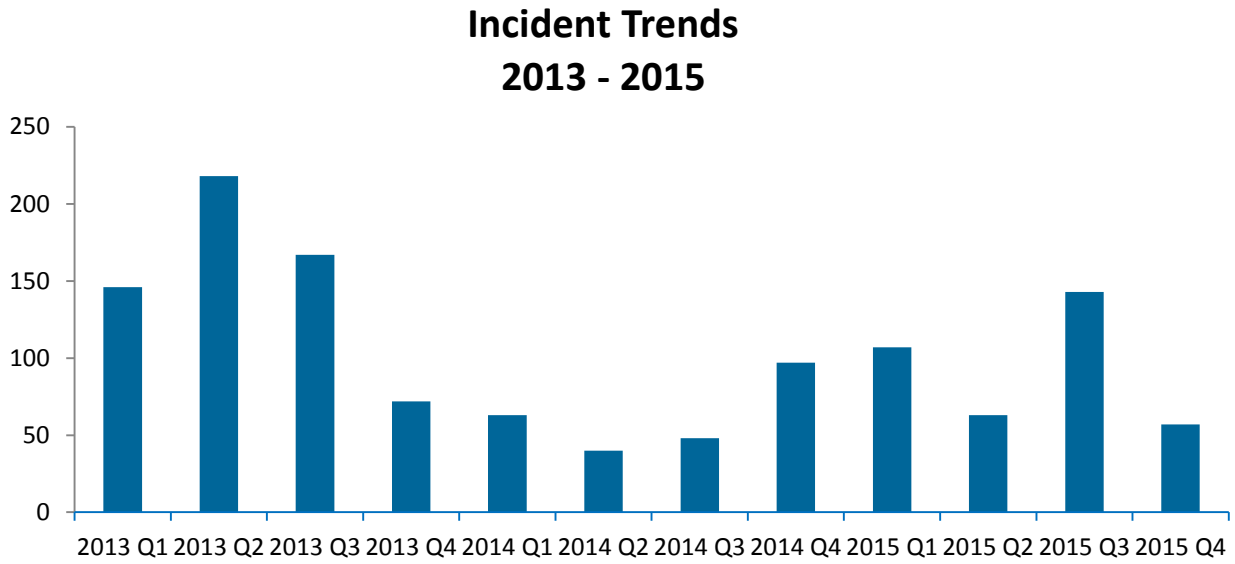
The *Code of Virginia*, *§2.2-603 (F)*, requires all executive branch agency directors to report IT security incidents to the CIO within 24 hours of discovery. The CSIRT then categorizes each security incident based on the type of activity.

CSIRT initiated a phishing campaign to evaluate the effectiveness of security awareness in the commonwealth. CSRM sent 40,896 COV simulated phishing emails to employees at 91

agencies. Of the emails sent, 21,632 (53 percent) were opened by the recipient. Of those who opened the emails, 5,384 (13 percent of sent emails and 25 percent of emails opened) clicked on the link inside the email. Another 3,348 users submitted their credentials in response to the phishing emails, representing 8 percent of all of the emails sent and 15 percent of the emails that were opened. This response indicated many employees in the commonwealth were aware of the risks associated with emails from an unknown sender. However, there is still a need to continue to educate employees on the dangers of opening and responding to emails from an unknown sender and raise information security awareness.

The data collected in 2015 shows that while the commonwealth is continually improving its security controls, IT systems remain a target of attack. This is illustrated by the increase of 49 percent from the prior year in the overall number of incidents. In the first quarter of 2015, the number of incidents increased slightly from the fourth quarter of 2014 due to a continuing phishing campaign against COV users. The campaign continued through February 2015. During the third quarter of 2015, there was a spike in the number of malware related incidents due to the Adobe Flash zero day vulnerabilities. These vulnerabilities were being exploited in the wild before patches were available. By the time Adobe released the patches, the exploits had been in the exploit kits for several weeks. Due to the criticality of these patches, CSRM was able to get them tested and deployed to COV devices in a little over two weeks, about half the time it takes for a normal patch cycle.

The increase in the number of incidents (to 370) remains a concern. In analyzing the indicators of compromise (IOC), CSRM discovered that attackers are utilizing different attack techniques. For example, phishing messages are being sent to other COV users from within the commonwealth, instead of outside of the commonwealth. COV employees demonstrated a tendency to trust other COV employees, and this resulted in an increase in unauthorized access to COV accounts.

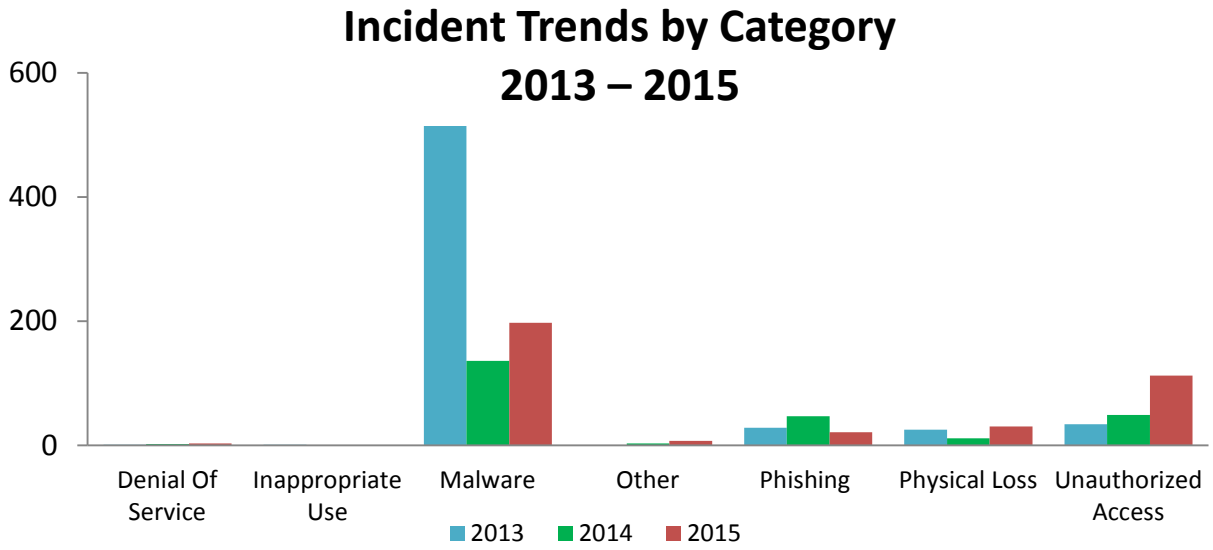


Incident Trends by Category

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.)

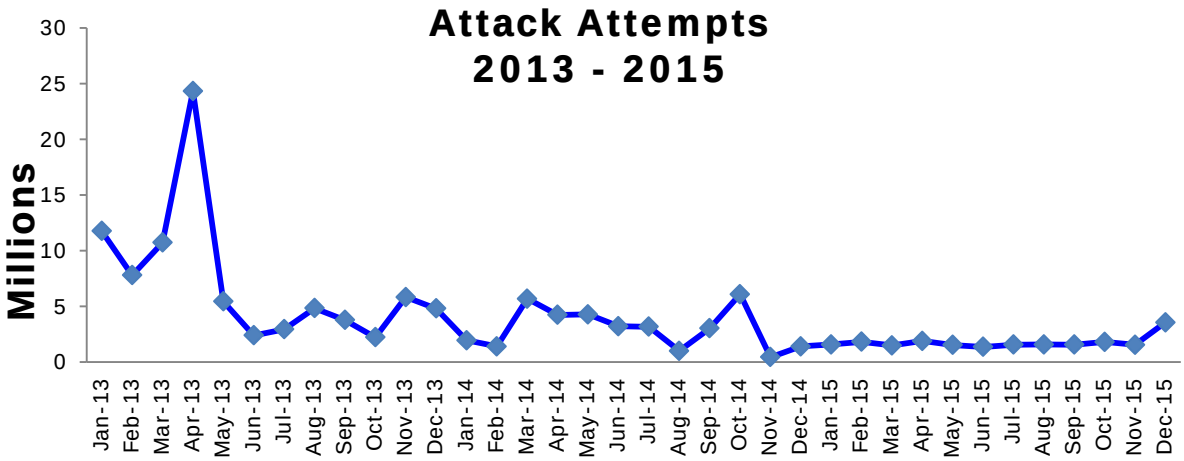
During 2015, malware infections continued to be the top category for security incidents. Attackers started utilizing ransomware to encrypt not only user desktops but attached network shares.



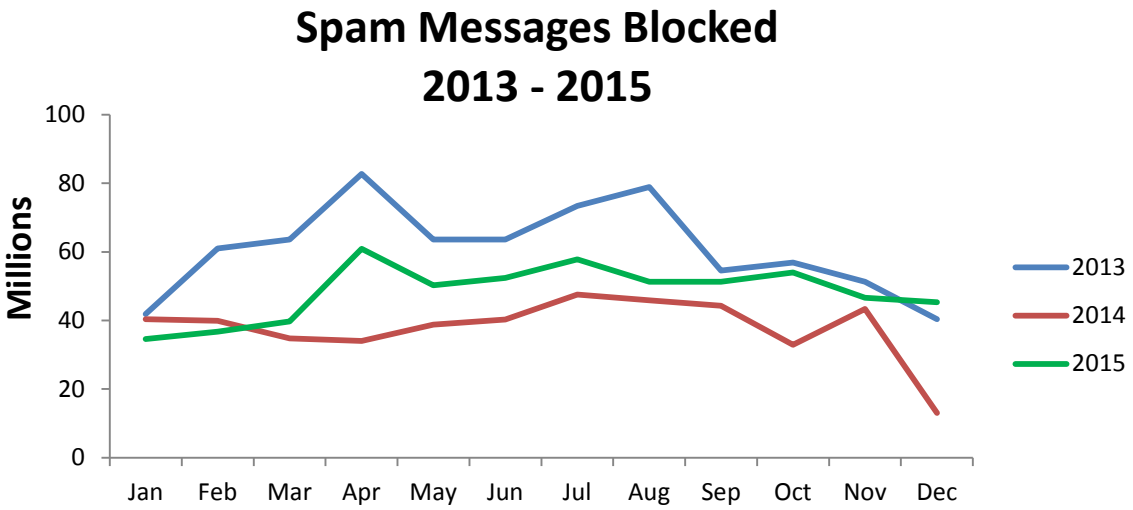
Note Use of compromised credentials in any attack, is categorized as unauthorized access.

The origins of the attacks on the commonwealth's network are monitored and tracked. While attackers often try to obscure their locations, this analysis indicated that the top five countries where attacks originated were the United States, China, Germany, Russia and France. This reveals the increasingly global nature of attacks on the commonwealth's networks and information. CSRM will continue to monitor the origins of these attacks and respond promptly to attacks on our networks, regardless of their origin.

Due to additional security controls put into place to filter out attacks, the overall number of attacks declined this year. The commonwealth received 21,128,109 alerts or approximately one attack every 1.5 seconds. While we strive to prevent attacks whenever possible, the number of new techniques and attempts continually challenges commonwealth IT security personnel to adapt quickly and defend against the constantly shifting cyber threat.



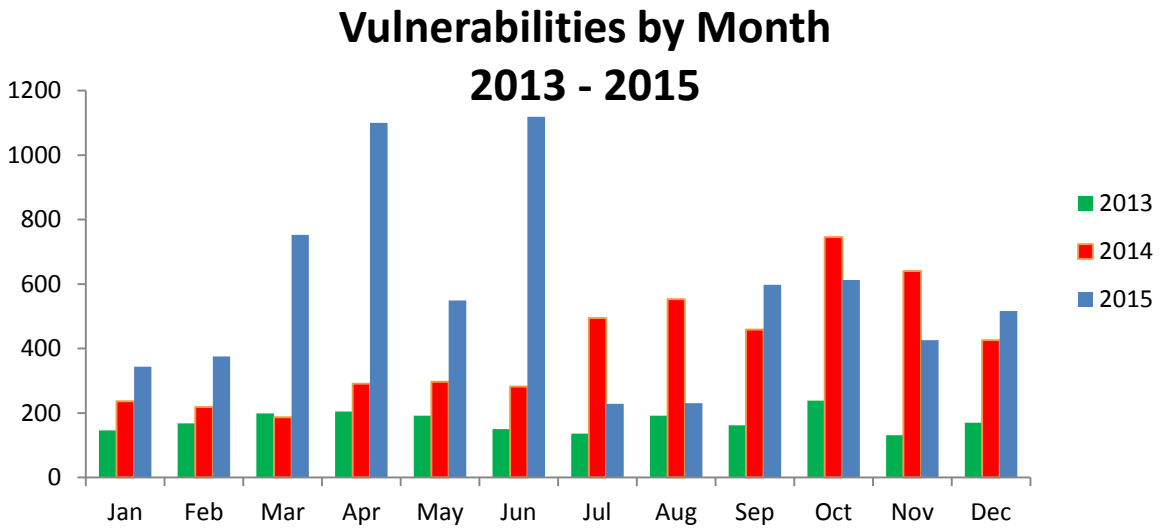
Email is an important part of commonwealth communication and is used almost everywhere to carry out daily business. Effective security tools must be in place to ensure malicious email activity is kept out of the enterprise environment as much as possible. Last year, the commonwealth filtered 581,051,302 spam messages and blocked 65,280 viruses from reaching commonwealth assets. The activity associated with both spam and viruses increased significantly from last year. While there isn't one source to which we can attribute this change, the increase is likely due to the rebuilding of a previously dismantled unsolicited email network.



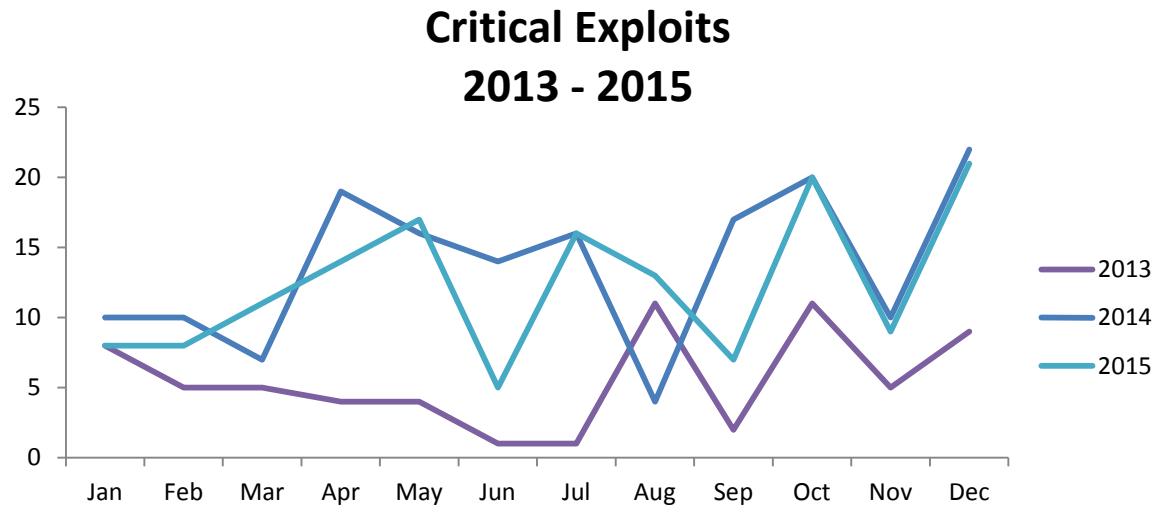
As part of tracking threats to the commonwealth, the CSIRT monitors COV systems for newly discovered vulnerabilities and incorporates them into a weekly advisory. This advisory is used by localities, state agencies and higher education. In 2015, the number of vulnerabilities increased by 42 percent from the prior year.

Several vulnerabilities in March through June that were of significant impact were the Adobe Flash zero day vulnerabilities and certificate vulnerabilities that occurred during that time. Due to vendor decisions not to patch the vulnerabilities associated with the Secure Sockets Layer (SSL) protocol, the technology was rendered obsolete and insecure, requiring the migration of SSL to Transport Layer Security (TLS). Presence of SSL technology is

widespread throughout the commonwealth IT enterprise, including web servers, network appliances and software applications on both servers and workstations. The process of replacing SSL with TSL requires significant resources in upgrading where optional and replacing where necessary, a substantial number of affected IT enterprise components.

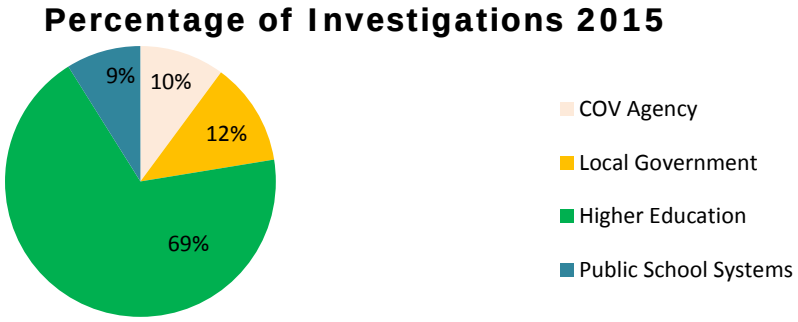


Of the vulnerabilities that were reported, there was a slight decrease in critical exploits, in 2015, the number of vulnerabilities decreased from 165 to 149, a 10 percent decrease. However, the number of incidents that were the result of these exploits had a major impact as seen in July through September when users were attacked using the Adobe Flash critical vulnerabilities. This is indicated by the number of malware incidents, which increased from 26 in the second quarter of 2015 to 107 in third quarter of 2015, an increase of 311 percent over the previous quarter.



Cyber Intelligence from Commonwealth Partners

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 MS-ISAC as potential events that they have monitored on the internet. CSRM disseminates the alerts to the affected entities and tracks them as investigations, since the results of the alert are unknown. In 2015, the commonwealth completed 412 investigations for the alerts that were received. This was a 78 percent increase over 2014. The following chart shows the percentage of investigations by type of entity.



Cyberattacks and other incidents at Virginia colleges and universities remain a significant risk. 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 their functions and the resources necessary to operate 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.

As summarized in the chart below, the data provided by MS-ISAC, higher education leads other public entities in the percentage of security investigations related to potential accounts compromised, malware infections, website defacement and cyberattacks. As these investigations are solely the investigations reported by MS-ISAC, there is potential for other security incidents to have been found and the potential for loss could be much greater. As a result, we recommend additional guidance for these institutions to ensure that appropriate governance is established and effective information security programs are implemented in higher education.

Security Investigations by Category

	Higher Ed	Local Government	Public School Systems	COV Agencies
Accounts Compromised	94%	2%	1%	3%
Malware Infections	93%	2%	1%	4%
Vulnerable Systems	33%	39%	13%	14%
Website Defacement	86%	14%	0%	0%
Cyberattacks (other)	50%	10%	0%	40%

	Higher Ed	Local Government	Public School Systems	COV Agencies
***Potential Loss Associated with Records Exposed**	$1,175,100	$10,404	$25,200	$9,792

*Potential loss associated with records exposed assumes records were exposed and was calculated using the Per Capita Cost of a Data Breach from the Ponemon Institute's 2015 Cost of a Data Breach Study: Global Analysis report and the number of security investigations.

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 (IS) Council and the commonwealth's Information Security Officers Advisory Group (ISOAG).

Statute Requires CIO to Identify Noncompliant Agencies

As directed by §2.2-2009 (B.1) 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

Threat Management Program

- Information identifying active threats to commonwealth data and systems
- Continuous monitoring analysis
- External actor threat monitoring

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 2015, CSRM reviewed and updated several policies.

- NIST 800-53 revision 4 and "Cybersecurity Framework" were incorporated into the security standard, SEC501-09. The update includes enhancements to controls for account management, disabling inactive accounts, security awareness training, continuous monitoring/trend analysis, configuration requirements for international travel and some administrative changes. The new document is more refined, takes into account feedback from ISOs, auditors and others, and provides for additional security measures to protect the commonwealth's information.
- CSRM also updated ITRM Standard SEC514-04 "Removal of commonwealth Data from Electronic Media" to add requirements for disposing of solid state media devices, flash-memory devices and multi-function devices. This revision also addressed future technologies and the need for an appointed individual to be responsible for the electronic data removal process.
- CSRM also began work on "Hosted Environment Information Security Standard" (SEC525-01). This standard was designed to establish a baseline for information security and risk management activities associated with commonwealth data stored in a data center not owned or leased by the Commonwealth of Virginia, including cloud storage solutions. The proposed standard was intended to direct agencies to ensure that the appropriate information security and risk management activities were performed to provide protection of, and mitigate risks to agency information systems stored at a third party hosting provider. Additional federal governance is needed to address third party hosted systems. CSRM will continue to monitor the security governance requirements in this area, as well as develop and implement additional standards regarding cloud security and the cloud security model where needed.

Additional controls were implemented to enhance accountability for information security program compliance. CSRM plays a role in the IT investment review process to help ensure that the security of the commonwealth's data is evaluated as a part of the procurement process. An additional requirement was implemented to discourage agencies that had inadequate information security audit programs from beginning new technology projects, including new information security investments and off premise hosting requests, until they addressed their existing information security issues and risks. This effort was designed to help agencies prioritize funding and resources to address existing information security

concerns before beginning new projects. As agencies migrate to third party vendors that provide software specific services, their IT security programs have become more critical to protect the confidentiality, integrity and availability of the commonwealth's data. Most agencies currently aren't equipped with resources or technology to handle the additional oversight and/or responsibilities required to provide adequate monitoring of these vendors. As a result, CSRM continues to work with agencies to understand their risk posture and determine secure solutions. To further support the agencies, VITA will be standing up third party hosting services in 2016 to provide an additional service solution to the commonwealth.

VITA developed an effective approach to address information security program weaknesses. The governor's issuance of Executive Directive 6, "Expanding Cyber-related Risk Management Activities" required VITA to provide an updated inventory of all data and computer systems. This inventory included the determination of sensitivity and criticality of systems and data, risk prioritization and scope of systems and data, and development of a risk-based approach to enhance the protection of systems and data. As a result, CSRM surveyed the agencies to determine the nature of the applications and data maintained by the agency. For systems that were determined to be sensitive, CSRM obtained additional information security and operations management information to evaluate the controls and risks to commonwealth data. In addition, the directive required VITA to recommend strategies to strengthen and modernize agencies' cybersecurity profiles. Based on the results, CSRM determined that the number of sensitive systems in the commonwealth increased from 740 systems to approximately 1,700 sensitive systems. As VITA begins to provide agency ISO services, we anticipate that resources will be allocated appropriately to evaluate these systems and assess their information security risk.

In addition, the General Assembly introduced legislation to establish an IT security service center operated by VITA. The proposed service center would provide security services, including vulnerability scans, IT security audits, risk management and other IT security services to executive branch agencies to support the effectiveness of agencies' information security programs. The proposal also gave VITA responsibility to conduct vulnerability scans of all public-facing websites and systems that are operated by state agencies. VITA is targeting the summer of 2016 to have services implemented to assist agencies with their information services program.

Small Agency ISO Program

The CSRM small agency ISO program assisted six new agencies in 2015 with their IT security programs. The program also continued to provide IT security services for the eight agencies that were initially contacted in 2014.

The areas of assistance for the designated agencies focused on:

- Providing documentation for the business impact analysis, formulating the risk assessment, and preparing the IT security risk assessment and audit plan for six agencies;
- Providing documentation for the IT risk assessment plan and IT security audit plan at three agencies;
- Assisting with the preparation of a business impact analysis at four agencies; and
- Assisting with the preparation of IT security policies and procedures for two agencies.

For the agencies assisted, based on the average 2015 data point scores, we noted a 17 percent improvement in the overall audit program and a 30 percent improvement of the overall risk profile over the average 2014 data point scores for the agencies.

The small agency ISO program provided assistance to five small agencies to collect the system documentation that determined sensitivity and criticality for their data in accordance with Executive Directive 6.

During 2015 CSRM was also tasked with obtaining the dataset information for Executive Directive 6 (2015) "Expanding Cyber-Related Risk Management Activities." The small agency ISO program was a critical component to understanding the data hosted at small agencies.

CSRM's small agency ISO program continued to obtain agency system information for the implementation of the IT security audit services program. In all, 28 agencies were contacted by the small agency ISO program and were provided assistance for obtaining audit quotes for their sensitive systems. For the agencies that were contacted by the small agency ISO program, one agency had their sensitive systems audited prior to the end of 2015 and another agency plans to obtain IT security audit services prior to July 1, 2016.

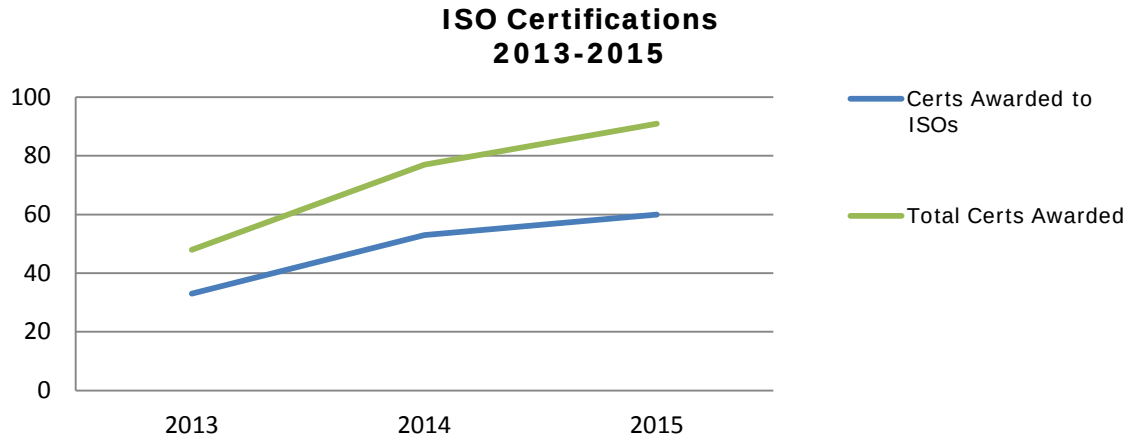
Commonwealth Information Security Council

The commonwealth 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 bi-monthly to provide direction for the commonwealth's information security program, and formed committees to address the following initiatives for 2015:

- The Second Annual Commonwealth of Virginia Information Security Conference: Council members planned and organized the conference for IT professionals throughout the commonwealth
- IT security standards and policies: Council members made recommendations for policy changes and updates
- ISO communication and knowledge sharing website: Council members manage the site to promote communication and information sharing between ISOs.

ISO Certification Program

CSRM administers the VITA ISO certification program. The agency ISOs are required to have formal training to demonstrate their understanding of the commonwealth's information security program. In 2015, 60 certifications were awarded to ISOs and 91 total certifications were awarded in 2015. This is a 90 percent increase from the number of certifications awarded in 2013. The increase in ISO certifications indicates greater awareness and understanding of the commonwealth security program.



Commonwealth Information Security Officers Advisory Group

The 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 security posture of the commonwealth. The members share best practices and knowledge through monthly meetings, are notified of opportunities to provide feedback on proposed policy changes, and receive 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 2015, ISOAG monthly meeting keynote speakers included representatives from government and various private sector organizations with expertise in information security.

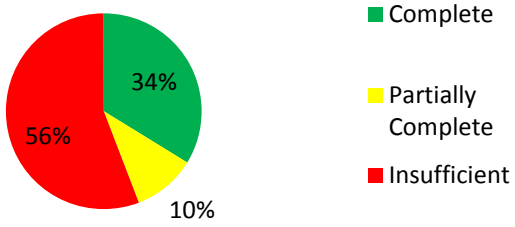
ISOAG meetings averaged 144 attendees per meeting, an increase from an average of 140 attendees per meeting last year. Members attended the meetings in person or via webinar. The option to attend the meetings via webinar was intended to help security professionals save travel time and cost. In addition, 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. Meeting materials are also posted to VITA website as an additional resource to employees.

Commonwealth Security Compliance Metrics

There was no significant improvement to information security audit program compliance in 2015. 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 carry out corrective action plans for findings noted during the audits. In 2015, while there was an increase in completed audit programs, the improvement is only slight as the increase appears to be related to a decrease in partially completed programs. These results indicate that agencies that have been on a path to improvement have made enough progress to maintain an adequate program. While this improvement is welcome, there was only a two percent decrease in the number of insufficient audit programs it the commonwealth.

Overall, only 34 percent of agencies have implemented a complete audit program. The lack of security audits continues to delay the development of an accurate assessment of the information security risk to commonwealth systems. With the proposed implementation of the information security services center, agencies will have additional resources available to perform these audits and identify information security risks to commonwealth systems and data.

Commonwealth Overall Audit Program Score



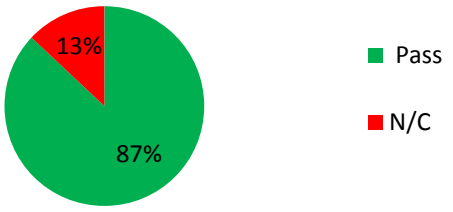
Overall audit program score completion increased by 10 percent

ISO certification is an important element of the commonwealth information security program. ISO certification demonstrates an understanding of information security risks and commitment to promoting information security in the commonwealth. This expertise and assurance is vital to lead the charge to protect the confidentiality, integrity, and availability of the commonwealth's data. In the agencies where the ISO is not certified, 96 percent of the overall audit programs are insufficient. The following agencies do not have certified ISOs:

- Tobacco Region Revitalization Commission (TIC)
- Virginia Resources Authority (VRA)
- Gunston Hall (GH)
- State Council of Higher Education Center (SCHEV)
- Virginia Commission for the Arts (VCA)
- Office of the Attorney General (OAG)
- Department for the Deaf and Hard of Hearing (DDHH)
- Virginia Foundation for Healthy Youth (VFHY)
- Commonwealth's Attorney's Service Council (CASC)
- Motor Vehicle Dealer Board (MVDB)

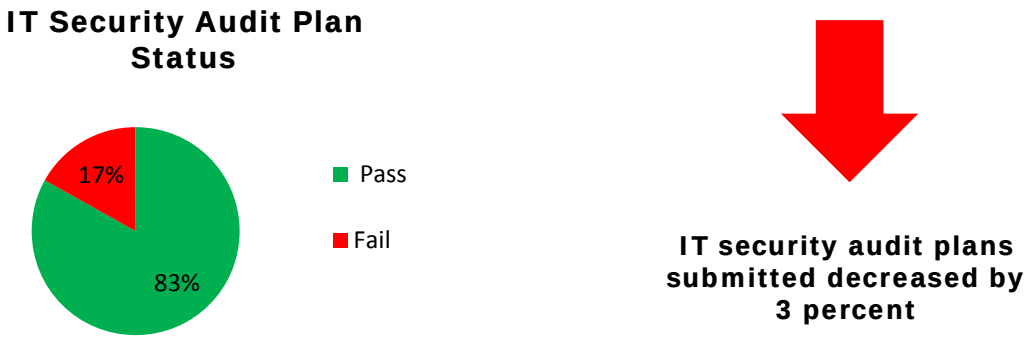
These agencies may be candidates for using the centralized ISO services that VITA will offer in 2016 to enhance the agencies' information security programs and support compliance with the commonwealth security standards.

ISO Certification Status



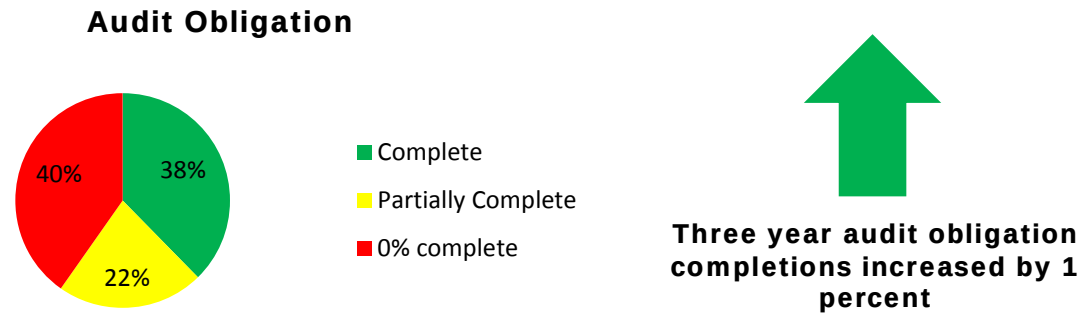
ISO certification increased by 1 percent

Most agencies have submitted a current IT security audit plan. Agency heads are accountable for their cybersecurity program. Part of this program includes a formal security controls review of agency sensitive systems. Each sensitive system at an agency must be audited at least once every three years as part of the periodic controls review. IT security audit plans also help provide input to an agency's official list of sensitive systems. The agency also will use this plan to 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. The commonwealth uses the security audits that result from the plan to determine if the proper controls exist and to evaluate them according to the requirements of the commonwealth Information Security Standards, federal laws, state laws and regulations.



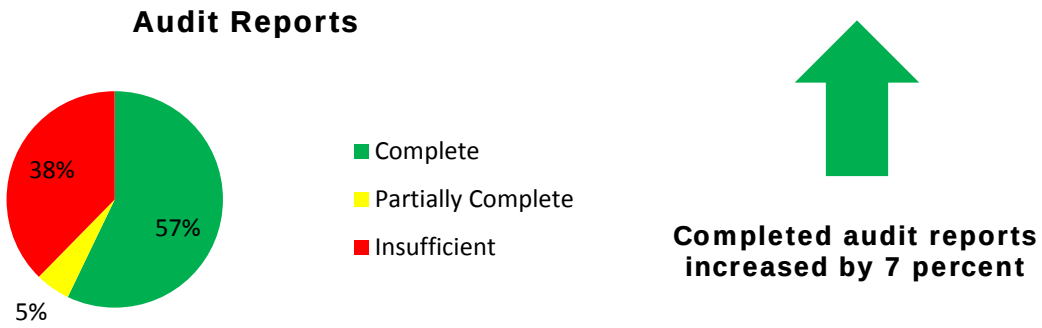
Most agencies did not complete required audits. As discussed, agency heads must ensure that each sensitive system is audited at least once every three years. The degree to which agency heads have fulfilled this audit obligation has been measured using the audit plans each agency submitted beginning in 2007.

Of the 77 agencies, 29 agencies (38 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 and audited some of their applications. Agencies should continue to strive toward meeting their audit obligations.



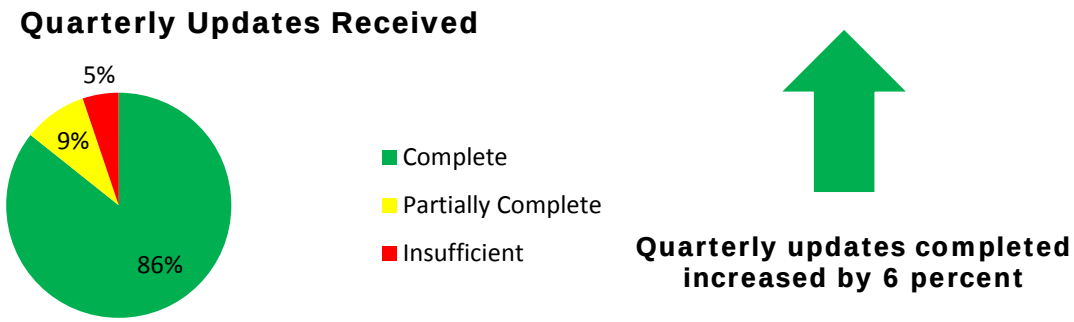
About half of the agencies submitted information security audits reports summarizing the review of their agencies IT systems' policies, records and activities. IT security audit reports document the results of the IT security audits. Audit results must be presented to the agency head or designee in a draft report for their review and comment. These results include IT security findings identified during the IT security

audit and recommendations and corrective actions that should occur to remediate the finding. IT security audit reports are required to be submitted to the CISO after the completion of a sensitive system IT security audit. Of the 77 agencies, 44 agencies were compliant. This included 25 agencies that did not have an audit report due.



Most agencies submitted 2015 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 all the corrective actions have been completed.

Of the 77 agencies, 32 agencies had quarterly updates due for open corrective action plans in 2015. Of those 32 agencies, 21 (66 percent) have submitted all updates; 7 agencies (22 percent) have submitted some of the updates; and 5 agencies (12 percent) have not submitted any updates. The summary includes 45 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. As a result, the chart below presents a misleadingly positive view of compliance.



IT security audits revealed key findings and related risks. Access control findings were the most frequent findings identified in the IT security audits. In 2015, 26 percent of all findings reported were related to access controls. These findings were typically associated with agency-specific applications, and indicate the need for an identity access management standard. CSRM currently is developing such a standard.

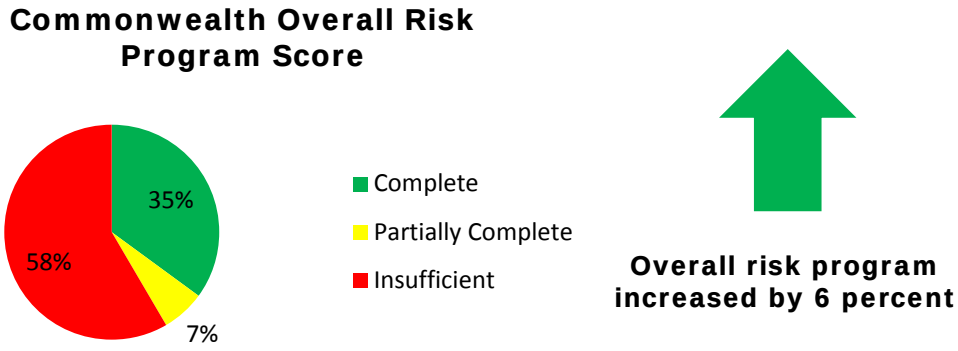
Risk assessments had the second highest number of findings, comprising 10 percent of all findings. Information gathered by the CSRM risk team indicates more than half of all agencies do not complete regular risk assessments. However the findings could be higher, because agencies have not been performing 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.

CSRM will be carefully monitoring critical findings in 2016 to ensure that those findings are remediated and their related risks are mitigated in a timely manner.

Commonwealth IT Risk Management Program

Commonwealth agencies continued to work on the submission of their business impact analyses (BIA), risk assessments and intrusion detection reporting. The number of agencies with completed risk program increased by 6 percent and the number of agencies with insufficient risk programs increased by 4 percent. Only the number of agencies with partially complete programs decreased. Progress is still needed in the planning and performance of sensitive IT system risk assessments to help ensure risks are adequately identified and managed in the commonwealth.

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 management program.



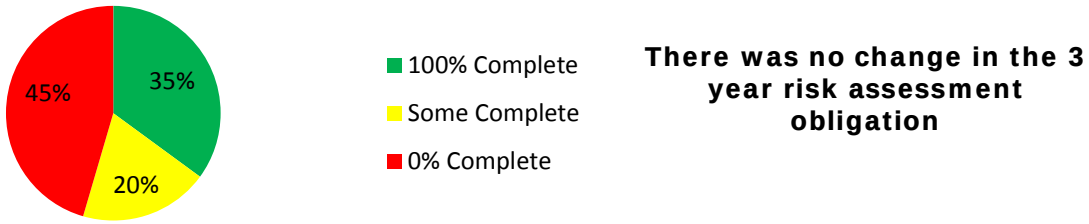
Agencies did not adequately use a BIA to document potential impacts of adverse information security events. A BIA delineates the steps necessary for agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions. With the proper information, the BIA can help to guide risk management activities. There were 56 agencies who submitted BIA information. Of those agencies, 43 (83 percent) provided complete BIA information. Included within the BIA are data classification and data sensitivity identification activities. The necessary criteria include:

- 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;
- Recovery 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.

Most agencies did not provide complete information to identify, analyze, and evaluate risk. Each agency is required to develop a risk assessment plan or review and as necessary, update an existing one for the IT systems for which it is the data owner on an annual basis. The risk assessment is the process of identifying vulnerabilities, threats, likelihood of occurrence and potential loss or impact. There were 26 agencies (34 percent) that provided complete risk assessment information. Of the 77 agencies, 51 agencies (66 percent) did not fully complete the required risk assessment information.

3 Year Risk Assessment Obligation



Vulnerability scans have not been completed sufficiently to adequately identify vulnerabilities that could threaten confidentiality, integrity or availability of systems. 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 2015, there were 42 agencies (55 percent) that performed all of the required application vulnerability scans on their sensitive, public-facing IT systems. This is an improvement from 2014, when 35 percent of agencies completed all of their required vulnerability scans. In total, 73 agencies (95 percent) reported some level of vulnerability scans were performed against their sensitive, public-facing IT systems, compared to 93 percent of agencies completing some level of vulnerability scans in the prior year. Four agencies (5 percent) did not submit any of the required vulnerability scans for their systems. VITA provides vulnerability scanning services for the agencies, but the applications remain largely untested. Attacks against public-facing web applications remain a primary method for attackers to gain unauthorized access to sensitive IT systems and data. To address this concern, CSRM will manage the vulnerability scanning for all public-facing web applications beginning in FY 2017 based on proposed legislation.

The threat metrics for most agencies were submitted to analyze the likelihood and magnitude of potential threats to the commonwealth's information. 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 77 agencies, 73 (94 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.

Cybersecurity Framework helps to assess commonwealth's security posture. The Cybersecurity Framework, a voluntary framework developed by NIST, is a tool that can help strengthen the commonwealth's ability to fight cybercrime and further enhance Virginia's position as a leader in cybersecurity. The 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 second 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. CSRM will continue to refine the data to provide additional insight into the current cybersecurity risk profile.

The 2015 cybersecurity framework 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

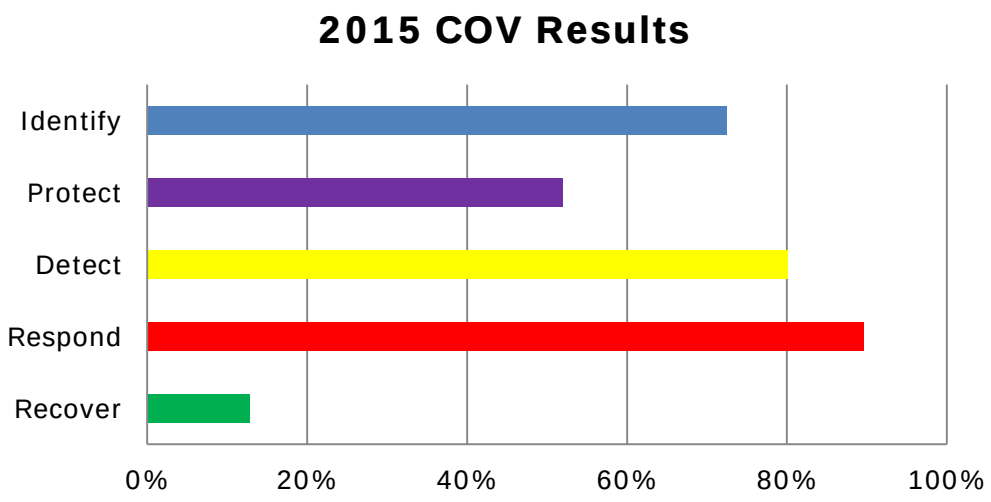
Respond: Develop and implement the appropriate activities, prioritized through the organization's risk management process, to take action regarding a detected information security event

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 information, the results of security audits and risk assessments to determine the maturity of each function. We will continue to evaluate these metrics as the information security processes and practices mature in the commonwealth. The following table identifies the data used to measure each function.

Function	Basis for Measurement	Target
IDENTIFY (ID)	Data set inventory, risk assessment (RA), and business impact analysis completed	100% - Indicates that a data set inventory, risk assessment, and business impact analysis were completed and approved by CRSM
PROTECT (PR)	ISO status, ISO certification, number of sensitive applications encrypted in transit, sensitive applications encrypted at rest, and number of applications using two factor	100% - Indicates agency identified an ISO, ISO was certified, applications were encrypted in transit, applications were encrypted at rest, and applications utilized two factor authentication
DETECT (DE)	Quarterly intrusion detection system (IDS) reports and vulnerability scanning	100% - Indicates when all four IDS reports were submitted with all required information and vulnerability scans performed for all necessary systems
RESPOND (RS)	Remediation plans for IT security audits	100% - Indicates remediation plans were developed
RECOVER (RC)	The time to remediate findings that were noted in information security audits	100% - Indicates that findings were closed in fewer than 180 days

The commonwealth's current risk posture is calculated based on results against target metrics. A summary of these metrics for the commonwealth is included in the 2015 COV Results chart below. The detailed listing of agencies and specific framework data points can be found in Appendix II.


2015 COV Results
Identify
Protect
Detect
Respond
Recover
0%
20%
40%
60%
80%
100%

Appendix I - Agency Information Security Data Points - Dashboard

Agency Information Security Data Points 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 is NOT certified.

2015 Overall Audit Program

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

2015 Overall Risk Profile

- All documentation received as requested information about the agency's vulnerability scans, business impact analysis (BIA), risk assessment(s) (RA)[1] and intrusion detection system (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

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

COV: Agency Data Points

Agency Name	Secretariat	Agency Acronym	ISO Designated	ISO Certification Status	Overall Audit Program	Overall Risk Profile
Alcoholic Beverage Control	Public Safety	ABC	Yes	Pass		
Board of Accountancy	Commerce and Trade	BOA	Yes	Pass		
Commonwealths Attorney's Services Council	Public Safety	CASC	Yes	N/C		
Compensation Board	Administration	CB	Yes	Pass		
Comprehensive Services for At-Risk Youth and Families	Health and Human Resources	CSA	Yes	Pass		
Department for Aging and Rehabilitative Services	Health and Human Resources	DARS	Yes	Pass		
Department of Behavioral Health and Developmental Services	Health and Human Resources	DBHDS	Yes	Pass		
Department of Criminal Justice Services	Public Safety	DCJS	Yes	Pass		
Department of Conservation and Recreation	Natural Resources	DCR	Yes	Pass		
Department for the Deaf and Hard of Hearing	Health and Human Resources	DDHH	Yes	N/C		
Department of Environmental Quality	Natural Resources	DEQ	Yes	Pass		
Department of Fire Programs	Public Safety	DFP	Yes	Pass		
Department of Forensic Science	Public Safety	DFS	Yes	Pass		
Department of Game and Inland Fisheries	Natural Resources	DGIF	Yes	Pass		
Department of General Services	Administration	DGS	Yes	Pass		
Department of Housing and Community Development	Commerce and Trade	DHCD	Yes	Pass		
Department of Health Professions	Health and Human Resources	DHP	Yes	Pass		
Department of Historic Resources	Natural Resources	DHR	Yes	Pass		
Department of Human Resource Management	Administration	DHRM	Yes	Pass		
Department of Juvenile Justice	Public Safety	DJJ	Yes	Pass		
Department of Military Affairs	Public Safety	DMA	Yes	Pass		
Department of Medical Assistance Services	Health and Human Resources	DMAS	Yes	Pass		

COV: Agency Data Points

Agency Name	Secretariat	Agency Acronym	ISO Designated	ISO Certification Status	Overall Audit Program	Overall Risk Profile
Department of Mines, Minerals and Energy	Commerce and Trade	DMME	Yes	Pass		
Department of Motor Vehicles	Transportation	DMV	Yes	Pass		
Department of Accounts	Finance	DOA	Yes	Pass		
Department of Aviation	Transportation	DOAV	Yes	Pass		
Department of Corrections	Public Safety	DOC	Yes	Pass		
Department of Education	Education	DOE	Yes	Pass		
Department of Forestry	Agriculture and Forestry	DOF	Yes	Pass		
Department of Labor and Industry	Commerce and Trade	DOLI	Yes	Pass		
Department of Planning and Budget	Finance	DPB	Yes	Pass		
Department of Professional and Occupational Regulation	Commerce and Trade	DPOR	Yes	Pass		
Department of Rail and Public Transportation	Transportation	DRPT	Yes	Pass		
Department of Social Services	Health and Human Resources	DSS	Yes	Pass		
Department of Veterans Services	Public Safety	DVS	Yes	Pass		
Department of Elections	Administration	ELECT	Yes	Pass		
Frontier Culture Museum of Virginia	Education	FCMV	Yes	Pass		
Gunston Hall	Education	GH	Yes	N/C		
Office of the Governor	Executive	GOV	Yes	Pass		
Indigent Defense Commission	Independent	IDC	Yes	Pass		
Center for Innovative Technology	Technology	IEIA	Yes	Pass		
Jamestown-Yorktown Foundation	Education	JYF	Yes	Pass		
Library of Virginia	Education	LVA	Yes	Pass		
Marine Resources Commission	Natural Resources	MRC	Yes	Pass		
Motor Vehicle Dealer Board	Transportation	MVDB	Yes	N/C		
Norfolk State University	Education	NSU	Yes	Pass		
Office of Attorney General	Executive	OAG	Yes	N/C		

COV: Agency Data Points

Agency Name	Secretariat	Agency Acronym	ISO Designated	ISO Certification Status	Overall Audit Program	Overall Risk Profile
Office of State Inspector General	Executive	OSIG	Yes	Pass		
Richard Bland College	Education	RBC	Yes	Pass		
Department of Small Business and Supplier Diversity	Commerce and Trade	SBSD	Yes	Pass		
State Corporation Commission	Independent	SCC	Yes	Pass		
State Council of Higher Education for Virginia	Education	SCHEV	Yes	N/C		
State Lottery Department	Independent	SLD	Yes	Pass		
Science Museum of Virginia	Education	SMV	Yes	Pass		
Southern Virginia Higher Education Center	Education	SVHEC	Yes	Pass		
Department of Taxation	Finance	TAX	Yes	Pass		
Department of Treasury	Finance	TD	Yes	Pass		
Tobacco Region Revitalization Commission	Commerce and Trade	TIC	Yes	N/C		
Virginia Commission for the Arts	Education	VCA	Yes	N/C		
Virginia College Savings Plan	Independent	VCSP	Yes	Pass		
Virginia Dept. of Agriculture and Consumer Services	Agriculture and Forestry	VDACS	Yes	Pass		
Virginia Department of Emergency Management	Public Safety	VDEM	Yes	Pass		
Virginia Department of Health	Health and Human Resources	VDH	Yes	Pass		
Virginia Department of Transportation	Transportation	VDOT	Yes	Pass		
Virginia Employment Commission	Commerce and Trade	VEC	Yes	Pass		
Virginia Economic Development Partnership	Commerce and Trade	VEDP	Yes	Pass		
Virginia Foundation for Healthy Youth	Health and Human Resources	VFHY	Yes	N/C		
Virginia Information Technologies Agency	Technology	VITA	Yes	Pass		
Virginia Museum of Fine Arts	Education	VMFA	Yes	Pass		
Virginia Museum of Natural History	Natural Resources	VMNH	Yes	Pass		
Virginia Resources Authority	Commerce and Trade	VRA	Yes	N/C		

COV: Agency Data Points

Agency Name	Secretariat	Agency Acronym	ISO Designated	ISO Certification Status	Overall Audit Program	Overall Risk Profile
Virginia Racing Commission	Commerce and Trade	VRC	Yes	Pass		
Virginia Retirement System	Independent	VRS	Yes	Pass		
Virginia School for the Deaf and Blind	Education	VSDB	Yes	Pass		
Virginia State Police	Public Safety	VSP	Yes	Pass		
Virginia State University	Education	VSU	Yes	Pass		
Virginia Workers Compensation Commission	Independent	VWC	Yes	Pass		

Agency Information Security Data Points Dashboard - Legend

Attended IS Orientation, Knowledge Center 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

2015 Audit Plan Status

Pass - Documents received as scheduled
N/C - Missing audit plan

2015 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

COV: Agency Data Points

Agency Secretariat	Agency 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	0%	100%	73%	Pass	82%	N/C	Pass	Pass
Commerce and Trade	BOA	Pass	Pass	100%	100%	100%	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	100%	N/A	100%	Pass	100%	Pass	Pass	Pass
Health and Human Resources	DARS	Pass	Pass	100%	100%	100%	N/C	N/C	Pass	Pass	Incomplete
Health and Human Resources	DBHDS	Pass	N/C	N/C	N/A	N/C	N/C	100%	Pass	Pass	Incomplete
Public Safety	DCJS	Pass	Pass	N/A	N/A	N/A	Pass	0%	Pass	Pass	Incomplete
Natural Resources	DCR	Pass	Pass	0%	100%	100%	Pass	100%	N/C	Pass	Incomplete
Health and Human Resources	DDHH	N/C	N/C	N/C	N/A	N/C	Pass	N/A	Pass	Pass	Pass
Natural Resources	DEQ	Pass	Pass	100%	25%	100%	Pass	0%	Pass	Pass	Pass
Public Safety	DFP	Pass	Pass	N/A	N/A	0%	Pass	0%	Pass	Pass	Incomplete
Public Safety	DFS	Pass	Pass	0%	N/A	0%	Pass	100%	Pass	Pass	Pass
Natural Resources	DGIF	Pass	Pass	0%	N/A	0%	Pass	7%	Incomplete	Pass	Incomplete
Administration	DGS	Pass	Pass	N/A	N/A	100%	Pass	0%	Pass	Pass	Pass
Commerce and Trade	DHCD	Pass	Pass	N/A	100%	0%	Pass	0%	Pass	Pass	Incomplete
Health and Human Resources	DHP	Pass	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass

COV: Agency Data Points

Agency Secretariat	Agency 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
Natural Resources	DHR	Pass	Pass	N/A	N/A	N/A	Pass	Pass	Pass	Pass	Pass
Administration	DHRM	Pass	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Public Safety	DJJ	Pass	N/C	N/C	N/A	N/C	Pass	0%	Pass	Pass	Incomplete
Public Safety	DMA	Pass	Pass	N/A	N/A	N/A	Pass	N/A	Pass	Pass	Pass
Health and Human Resources	DMAS	Pass	Pass	N/A	67%	79%	N/C	N/C	N/C	Pass	Pass
Commerce and Trade	DMME	Pass	Pass	0%	0%	0%	N/C	N/C	Pass	Pass	Incomplete
Transportation	DMV	Pass	Pass	0%	100%	9%	N/C	60%	N/C	Pass	Incomplete
Finance	DOA	Pass	N/C	N/C	100%	N/C	N/C	N/C	Pass	Pass	Pass
Transportation	DOAV	Pass	Pass	N/A	100%	100%	Pass	100%	Pass	Pass	Pass
Public Safety	DOC	Pass	Pass	17%	100%	67%	Pass	100%	Pass	Pass	Pass
Education	DOE	Pass	Pass	100%	100%	93%	Pass	0%	Pass	Pass	Pass
Agriculture & Forestry	DOF	Pass	Pass	100%	100%	65%	Pass	100%	Pass	Pass	Pass
Commerce and Trade	DOLI	Pass	Pass	N/A	N/A	0%	Pass	12%	Pass	Pass	Pass
Finance	DPB	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Pass
Commerce and Trade	DPOR	Pass	Pass	N/A	N/A	100%	Pass	100%	Pass	Pass	Pass
Transportation	DRPT	Pass	Pass	N/A	N/A	0%	N/C	N/C	N/C	Pass	Incomplete
Health and Human Resources	DSS	Pass	Pass	100%	67%	32%	Pass	0%	Incomplete	Pass	Incomplete
Public Safety	DVS	Pass	Pass	100%	N/A	100%	Pass	100%	Pass	Pass	Pass
Administration	ELECT	Pass	Pass	100%	N/A	100%	Pass	100%	Pass	Pass	Pass

COV: Agency Data Points

Agency Secretariat	Agency 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
Education	FCMV	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Education	GH	N/C	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Executive	GOV	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Pass
Independent	IDC	Pass	Pass	0%	N/A	N/A	Pass	100%	Pass	Pass	Fail
Technology	IEIA	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Pass
Education	JYF	Pass	Pass	0%	N/A	17%	Pass	17%	Pass	Pass	Pass
Education	LVA	Pass	Pass	0%	100%	67%	Pass	0%	Incomplete	Pass	Pass
Natural Resources	MRC	Pass	Pass	N/A	N/A	100%	Pass	100%	Pass	Pass	Pass
Transportation	MVDB	N/C	Pass	0%	N/A	0%	N/C	N/C	N/C	Pass	Incomplete
Education	NSU	Pass	N/C	N/C	N/A	N/C	N/C	N/C	Incomplete	Pass	Incomplete
Executive	OAG	N/C	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Fail	Incomplete
Executive	OSIG	Pass	Pass	100%	N/A	100%	Pass	N/A	Pass	Pass	Pass
Education	RBC	Pass	Pass	0%	0%	71%	N/C	N/C	N/C	Pass	Incomplete
Commerce and Trade	SBSD	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Independent	SCC	Pass	Pass	50%	100%	64%	Pass	0%	Incomplete	Pass	Pass
Education	SCHEV	N/C	Pass	N/A	0%	25%	N/C	N/C	N/C	Pass	Incomplete
Independent	SLD	Pass	Pass	0%	62%	67%	N/C	N/C	Incomplete	Pass	Fail
Education	SMV	Pass	Pass	N/A	N/A	0%	N/C	N/C	N/C	Pass	Pass
Education	SVHEC	Pass	Pass	N/A	N/A	N/A	Pass	N/A	Pass	Pass	Pass
Finance	TAX	Pass	Pass	100%	100%	97%	Pass	0%	N/C	Pass	Incomplete
Finance	TD	Pass	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Commerce and Trade	TIC	N/C	Pass	N/A	N/A	N/A	Pass	N/A	Pass	Pass	Incomplete

COV: Agency Data Points

Agency Secretariat	Agency 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
Education	VCA	N/C	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Independent	VCSP	Pass	Pass	100%	N/A	100%	Pass	100%	Pass	Pass	Pass
Agriculture & Forestry	VDACS	Pass	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Public Safety	VDEM	Pass	Pass	N/A	N/A	0%	N/C	N/C	Incomplete	Fail	Fail
Health and Human Resources	VDH	Pass	Pass	80%	100%	82%	N/C	N/C	N/C	Pass	Incomplete
Transportation	VDOT	Pass	Pass	100%	100%	100%	Pass	82%	Incomplete	Pass	Pass
Commerce and Trade	VEC	Pass	Pass	0%	75%	35%	N/C	N/C	N/C	Fail	Fail
Commerce and Trade	VEDP	Pass	Pass	N/A	N/A	0%	N/C	N/C	N/C	Fail	Pass
Health and Human Resources	VFHY	N/C	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Technology	VITA	Pass	Pass	0%	75%	100%	Pass	84%	Pass	Pass	Pass
Education	VMFA	Pass	Pass	0%	0%	0%	N/C	N/C	N/C	Pass	Pass
Natural Resources	VMNH	Pass	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Incomplete
Commerce and Trade	VRA	N/C	N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Incomplete
Commerce and Trade	VRC	Pass	Pass	N/A	N/A	N/A	Pass	N/A	Pass	Pass	Pass
Independent	VRS	Pass	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Education	VSDB	Pass	N/C	N/C	N/A	N/C	N/C	N/C	Incomplete	Pass	Incomplete
Public Safety	VSP	Pass	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Education	VSU	Pass	Pass	67%	47%	60%	Pass	9%	Pass	Pass	Pass
Independent	VWC	Pass	Pass	100%	N/A	100%	Pass	100%	Pass	Pass	Pass

COV: Agency Data Points

Appendix II- Cybersecurity Framework – Dashboard

Agency Acronym	Agency	Identify	Protect	Detect	Respond	Recover
CB	Compensation Board	33%	60%	75%	100%	0%
DGS	Dept of General Services	100%	100%	100%	100%	0%
DHRM	Dept of Human Resource Management	33%	90%	75%	100%	0%
ELECT	Dept of Elections	100%	68%	100%	100%	100%
DOF	Dept of Forestry	100%	61%	100%	100%	19%
VDACS	Virginia Dept of Agriculture and Consumer Services	100%	40%	100%	100%	61%
BOA	Board of Accountancy	100%	80%	100%	100%	0%
DHCD	Dept of Housing and Community Development	100%	70%	75%	100%	0%
DMME	Dept of Mines, Minerals and Energy	67%	40%	75%	0%	0%
DOLI	Dept of Labor and Industry	100%	78%	100%	100%	0%
DPOR	Dept of Professional and Occupational Regulation	100%	67%	100%	100%	0%
SBSD	Dept of Small Business and Supplier Diversity	100%	55%	75%	100%	0%
TIC	Tobacco Indemnification Commission	100%	20%	75%	100%	0%
VEC	Virginia Employment Commission	0%	40%	0%	75%	0%
VEDP	Virginia Economic Development Partnership	33%	67%	50%	100%	0%
VRA	Virginia Resources Authority	17%	20%	75%	100%	0%
VRC	Virginia Racing Commission	100%	40%	100%	100%	0%
DOE	Dept of Education	100%	41%	100%	100%	33%
FCMV	Frontier Culture Museum of Virginia	67%	40%	75%	100%	0%
GH	Gunston Hall	100%	20%	75%	100%	0%
JYF	Jamestown-Yorktown Foundation	100%	67%	100%	100%	0%
LVA	Library of Virginia	83%	43%	100%	100%	100%
NSU	Norfolk State University	17%	41%	75%	100%	0%
RBC	Richard Bland College	33%	65%	75%	0%	0%
SCHEV	State Council of Higher Education for Virginia	33%	60%	75%	0%	0%
SMV	Science Museum of Virginia	33%	50%	100%	100%	0%
SVHEC	Southern Virginia Higher Education Center	100%	40%	100%	100%	0%
VCA	Virginia Commission for the Arts	17%	20%	75%	100%	0%
VMFA	Virginia Museum of Fine Arts	33%	86%	100%	0%	0%
VSDB	Virginia School for the Deaf and Blind	50%	40%	75%	100%	0%
VSU	Virginia State University	100%	48%	100%	47%	8%
GOV	Office of the Governor	100%	53%	100%	100%	0%
OAG	Office of Attorney General	0%	20%	25%	100%	0%
OSIG	Office of State Inspector General	100%	40%	50%	100%	0%
DOA	Dept of Accounts	67%	57%	100%	100%	0%
DPB	Dept of Planning and Budget	100%	44%	100%	100%	0%
TAX	Dept of Taxation	50%	80%	75%	100%	42%
TD	Dept of Treasury	100%	49%	100%	100%	100%
CSA	Comprehensive Services for At-Risk Youth and Families	100%	60%	100%	100%	0%
DARS	Dept for Aging and Rehabilitative Services	67%	72%	75%	76%	11%
DBHDS	Dept of Behavioral Health and Development Services	50%	40%	75%	100%	0%
DDHH	Dept for the Deaf and Hard of Hearing	100%	20%	100%	100%	0%
DHP	Dept of Health Professions	100%	80%	55%	100%	80%
DMAS	Dept of Medical Assistance Services	33%	44%	100%	67%	0%
DSS	Dept of Social Services	83%	59%	55%	67%	78%
VDH	Virginia Dept of Health	33%	93%	100%	100%	48%
VFHY	Virginia Foundation for Healthy Youth	0%	20%	94%	100%	0%
IDC	Indigent Defense Commission	100%	40%	100%	100%	0%
SCC	State Corporation Commission	67%	40%	100%	100%	0%
SLD	State Lottery Dept	17%	40%	71%	62%	0%
VCSP	Virginia College Savings Plan	100%	62%	64%	100%	100%
VRS	Virginia Retirement System	100%	56%	83%	100%	0%
VWC	Virginia Workers Compensation Commission	100%	75%	100%	100%	0%
DCR	Dept of Conservation and Recreation	67%	70%	71%	100%	0%
DEQ	Dept of Environmental Quality	100%	40%	88%	25%	0%
DGIF	Dept of Game and Inland Fisheries	83%	47%	36%	100%	0%
DHR	Dept of Historic Resources	100%	80%	58%	0%	0%
MRC	Marine Resources Commission	100%	64%	55%	100%	0%
VMNH	Virginia Museum of Natural History	100%	50%	100%	100%	0%
ABC	Alcoholic Beverage Control	50%	47%	99%	100%	0%
CASC	Commonwealths Attorney's Services Council	0%	20%	71%	100%	0%
DCJS	Dept of Criminal Justice Services	100%	80%	71%	100%	0%
DFP	Dept of Fire Programs	100%	40%	84%	100%	0%
DFS	Dept of Forensic Science	100%	40%	92%	100%	0%
DJJ	Dept of Juvenile Justice	100%	40%	55%	100%	0%
DMA	Dept of Military Affairs	100%	40%	76%	100%	0%
DOC	Dept of Corrections	100%	75%	71%	100%	0%
DVS	Dept of Veterans Services	100%	80%	83%	100%	100%
VDEM	Virginia Dept of Emergency Management	50%	40%	100%	100%	0%
VSP	Virginia State Police	100%	54%	55%	100%	40%
IEIA	Center for Innovative Technologies	83%	40%	77%	100%	0%
VITA	Virginia Information Technologies Agency	67%	40%	55%	75%	0%
DMV	Dept of Motor Vehicles	33%	51%	90%	100%	0%
DOAV	Dept of Aviation	100%	48%	83%	100%	0%
DRPT	Dept of Rail and Public Transportation	33%	40%	30%	100%	0%
MVDB	Motor Vehicle Dealers Board	33%	30%	75%	100%	0%
VDOT	Virginia Dept of Transportation	67%	40%	68%	100%	65%