Virginia Information Technologies Agency

VITA

2013 Commonwealth of Virginia Information Security Report

www.vita.virginia.gov

Prepared and Published by:

Virginia Information Technologies Agency

Comments on the
2013 Commonwealth of Virginia Information Security Report
are welcome
Suggestions may be conveyed electronically to
CommonwealthSecurity@vita.virginia.gov

Please submit written correspondence to:

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

Virginia Information Technologies Agency

Contents

Executive Summary

This 2013 Commonwealth of Virginia (COV) Information Security Report is the sixth 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 independent and executive branch agencies, including Tier I institutions of higher education. This report does not address Tier III and Tier II institutions that have been statutorily exempted from compliance with Commonwealth policies and standards.

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

Agency business applications remain the primary attack vector within state government. Although agencies that use VITA's enterprise-wide infrastructure services have enterprise grade controls and security best practices for infrastructure services, each agency remains statutorily responsible for implementing security controls for their unique applications and data. However, agencies are not implementing the controls needed to protect their data and ensure only authorized personnel can access the applications. Controls for these applications are not evenly applied, and agencies have historically reported insufficient resources to remediate identified vulnerabilities. The lack of security controls on agency-specific applications contributes significantly to the malicious attacks that cause the most impact.

Those agency-specific systems and infrastructure that are not protected by VITA's enterprise services face an increased risk of attack. Similar to business applications, many agencies operate unique IT systems that are not supported or protected by VITA's enterprise services. Many of these agency-specific systems support critical infrastructure, and agencies need to secure them by ensuring that effective security controls are in place. However, agencies often do not protect their systems to the same degree as VITA's enterprise infrastructure, putting parts of the Commonwealth's 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, that contain computers and applications which support critical infrastructure such as transportation and public safety. The Hampton Roads area serves as an example of an area where bridges and tunnels could cripple the local area, should the supporting IT infrastructure be compromised.

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 compromise: The Virginia State Police, the Virginia Department of Emergency Management, and the Virginia Employment

Commission. 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. These agencies need to complete transformation as soon as possible.

Corrective action is required in 2014 to remediate a continued reduction in the percentage of agencies that complete their audit obligations. For the past three years, the majority of agencies have failed to meet minimum requirements for auditing their sensitive systems. Commonwealth security standards require each agency to audit their sensitive systems at least once every three years. However, in 2011 and 2012 only 43 percent of agencies met this requirement. This compliance rate dropped in 2013, falling to 33 percent. Accordingly, the CIO may be required to exercise his obligation to order security audits be performed for these agencies per § 2.2-2009 of the *Code of Virginia*.

Inadequate access control was the number one issue found in risk-based evaluations, comprising 20 percent of all security audit findings. Access control risk is widespread, with 55 percent of all agencies that submitted audits reporting at least one access control related finding. Ninety-nine percent of all findings were rated high by the agencies, based on industry standards. These findings were typically associated with agency-specific applications and indicate the need for an identity access management standard which would provide guidance in the remediation of these findings.

Evidence suggests that higher education institutions are at greater risk for cyber attacks and other incidents. In Virginia, institutions with management agreements are statutorily exempt from VITA's oversight, but they are still 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.

The Commonwealth significantly reduced the number of successful attacks within the enterprise in 2013. Operational changes such as a reduction in the number of devices with elevated privileges, and patching of commonly used software, drove the reduction in security incidents. These reductions required a substantial degree of communication, coordination, and cooperation between agencies and VITA. Going forward, improvements in these areas will be needed in order to effectively and rapidly remediate future threats.

In 2013, Commonwealth agencies made improvements, both in the quantity and quality of business impact analysis (BIA), risk assessment and intrusion detection reporting. The most noticeable improvement was a 21 percent increase in BIA submissions over the previous year. While noticeable improvements were made in the Commonwealth's risk management program in 2013, the IT Risk Management Standard introduced additional risk management activities for agencies to address. The Commonwealth's risk management posture has improved since 2012, but significant work remains. CSRM anticipates continued improvement in the risk management program data as processes mature.

The Commonwealth's new information security officer (ISO) certification program had a promising start and has provided a strong baseline upon which to build. Fifty-two of the 76 designated primary ISOs established a common educational background in information security specific to the commonwealth. With 88 percent of ISOs participating in training and discussions, Virginia's ISOs are now better equipped to tackle the challenges of protecting their agencies.

The past year has seen progress in some areas, however a number of issues included in the 2012 report still remain. In 2013, CSRM integrated the requirements of the National Institute of Standards and Technology (NIST) CyberSecurity Framework into the Commonwealth's IT Risk Management Standard. In doing so, the Commonwealth became the first state in the nation to adopt the NIST framework and report results. In addition, CSRM saw an increase in awareness about our information security program (due to increased participation in the ISO certification program and the advisory group), a heightened understanding of the impacts of security risks, and an increase in the number of attacks against Commonwealth systems that were successfully mitigated.

However, the lack of attention by agencies to the security audit program continues to put the Commonwealth at risk, and the lack of insight into untransformed and out-of-scope agencies and systems continues to present the Commonwealth with an elevated level of risk. These concerns could be reduced by ensuring that the information security program is consistently applied to all Commonwealth systems, and by requiring broader compliance with IT security and risk management standards and policies. CSRM is assessing methods for restructuring and possibly centralizing the information security audit program in order to improve the information security audit program in the Commonwealth.

2013 COV Information Security Program

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

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

Audits

- 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

Risk

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

Operations

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

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

- Preventing cyber attacks against the Commonwealth's critical infrastructures
- Prevent theft of Commonwealth data
- Reduce the Commonwealth's vulnerability to cyber attacks
- Increase the Commonwealth's ability to respond quickly and effectively against cyber attacks, minimizing damage and recovery time

- Establish a cybersecurity knowledgeable workforce
- Establish cybersecurity resources at Commonwealth agencies
- Improve cybersecurity situational awareness
- Identify and remediate risks to Commonwealth data
- Establish IT infrastructure impact analysis

In the second quarter of 2013, CSRM implemented a governance risk and compliance tool, designed to improve analysis and reporting. This tool will aid CSRM in correlating business information against agency infrastructure and impact. This comprehensive risk picture can then be communicated to agencies, real-time.

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 work includes providing input to revisions of VITA's standards, and providing messages for Information Security Awareness Month in October for inclusion in the Governor's Leadership Communiqué. The IS Council meets monthly to provide direction for the Commonwealth's information security program, and formed committees to address the following three initiatives for 2013:

- Bring-Your-Own-Device security strategy
- ISO manual
- Information security conference

Due to continued participation within the information security community, the IS Council has developed the following 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

Information Security Policies, Standards and Guidelines

The Commonwealth's IT security program is comprised of one policy and five standards designed to assist agencies in building and documenting their security program. The policy sets the Commonwealth's overall direction and establishes a framework that agency heads must follow in implementing IT security programs. 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 that does not comply with the requirements.

In 2013, CSRM focused on further development of the risk management program and additional refinement of existing security controls. The risk management program development included work to formalize risk management language and procedures as well as integration of the National Institute of Standards and Technology (NIST) cybersecurity framework. The Commonwealth became the first state in the nation to adopt the framework and report results. In addition to the risk management standard the Commonwealth updated the security controls standard to include updates to logical access requirements. In the coming year CSRM will focus on updating Commonwealth standards to align with the newest revision of the NIST security control standard. CSRM has made policy templates available to the agencies to reduce the number of resources required for implementation of these changes.

Also in line with recent NIST publications, CSRM developed a risk management standard that gives the Commonwealth a framework for assessing and documenting risk. This standard provides a common method of describing an agency's current risk management posture and target risk management state, identifying and prioritizing opportunities for improvement within information security and risk management programs, assessing progress toward the target risk state, and reporting risk management postures and activities.

Based on data included in prior annual reports, small agencies were identified as more likely to have an insufficient information security program. In order to help address this risk, CSRM implemented a program to assist small agencies in the documentation of their information security program. The small agency program focuses on developing the core information security documents that allow an agency to identify their most significant risks and develop a plan for the agency to review their environment for additional risks in the future. These core documents are created in conjunction with agency business representatives in order to properly reflect agency needs. The primary areas of focus will include a business impact analysis, identification of sensitive systems, formulation of a risk assessment, and preparation of the IT security audit plan. The program has initially focused on agencies with fewer than 50 full-time employees who have been unable to provide the resources for maintaining their information security program. Eight agencies have been identified for assistance in 2014.

Higher Education

One of Virginia's greatest assets is the number of strong public higher education institutions. These institutions not only graduate educated professionals, they 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.

In 2010, cyber criminals transferred funds just shy of $1 million from a higher education institution in Virginia. In 2013, one of Virginia's colleges had a data breach that compromised information submitted by almost 150,000 job applicants. More recently, the University of Maryland reported a breach that compromised over 300,000 personal records including names, date of birth, and Social Security numbers, dating back to 1998. These examples reinforce the importance of effective security controls and governance in higher education.

There has been a recent trend over the last few years where higher education institutions are statutorily excluded from compliance with the Commonwealth's information security program standards and reporting. Due to the number of higher education breaches that have been publicized both within the Commonwealth and from other states, CSRM recommends that a third party entity create a common set of security, governance requirements and a corresponding annual report, similar to this report, to identify higher education institutions that have not implemented acceptable policies, procedures and standards.

Control Systems and Critical Infrastructure

Within the last year, there has been an increase in the identified vulnerabilities in control systems, sometimes referred to as Supervisory Control and Data Acquisition (SCADA) systems. These devices often support critical infrastructure, and bridge the digital and physical worlds by managing everything from prison doors to bridge openings. Due to the design and function of the systems, they often do not have security controls in place and thus are vulnerable to cyber security threats. The concerns posed by those inherent risks are especially acute given the need to remotely access control systems during emergencies. Accordingly, control systems are a frequent target of malicious third parties.

Examples of the importance of control systems, and their inherent vulnerabilities, are growing more abundant and acute. In June of 2012, a mid-Atlantic Derecho disrupted power to about one million homes in Virginia. The storm had a state-wide impact, and affected operations at data centers, telephone switching offices, emergency 911 services, and roadways. Although this was not a malicious attack, it still crippled our critical infrastructure. By contrast, a targeted attack has the potential to inflict damage of the same or greater magnitude. While the number of attacks on critical systems are not often publicized several significant examples are publically known. In February 2013, an attacker compromised an emergency alert system in Montana and broadcast a fake emergency situation. In late 2013, cyber researches released information showing that over 10,000 satellites were vulnerable to exploits. These satellites control everything from retail terminals to energy sector systems. If an attacker were to find similar vulnerabilities in the Commonwealth's critical infrastructure, whether using traditional network connections or satellite communications, they could cause some significant damage. The Hampton Roads area serves as an example of an area where changing the traffic flow of bridges and tunnels could cripple the local area should the supporting IT infrastructure be compromised. HVAC systems, air pumps, traffic signals, emergency lights, and any other system that was designed to be remotely monitored and controlled could be compromised.

State agencies use control systems to support many critical services that support and protect citizens. Historically, agencies have often regarded these systems as exempt from VITA's oversight because they are not part of VITA's enterprise infrastructure services. These systems are not, however, exempt from Commonwealth security policies and standards. Moreover, these systems pose a high risk to the Commonwealth because they support Commonwealth-owned critical infrastructure. CSRM will investigate whether additional security reviews and controls should be added for those control systems that support the critical operations and infrastructure of the Commonwealth.

Commonwealth Information Security Officer's Advisory Group

The Commonwealth of Virginia's Information Security Officers Advisory Group (ISOAG) is a dynamic group open to all government personnel. The focus is IT security knowledge exchange to improve the posture of the commonwealth. The members share best practices and knowledge through monthly meetings and timely security alerts provided by CSRM. The group interacts with national and state experts and receives updates to the Commonwealth's information security program. Members are also frequently notified of cybersecurity training opportunities in the region. In 2013, ISOAG monthly meeting keynote speakers included representatives from NIST, US Immigration and Customs Enforcement, Old Dominion University, Department of Motor Vehicles, Department of Corrections, Virginia College Savings Plan, Federal Reserve Bank, Federal Bureau of Investigations, Innovation and Entrepreneurship Investment Authority, and various private sector organizations with expertise in information security.

ISOAG membership has grown from approximately 200 members in its inaugural year (2008) to 583 members at the end of 2013. 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 strong attendance of 1,610 attendees: an average of 134 attendees per meeting. 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.

Information Security Orientation

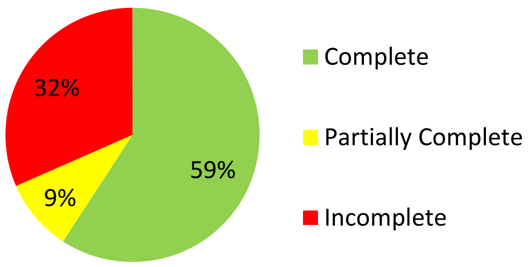
The information security orientation program is an opportunity for agency personnel with IT security roles and responsibilities to gain a better understanding of the commonwealth's security framework. Orientation includes a discussion of IT security in the commonwealth, standard best practices, available resources, compliance, and a walk-through of how to build and document an agency program. As part of the orientation improvement in 2013, CSRM introduced the use of audience response devices for in-person and online participants. The devices facilitated a more interactive session and allowed instant and insightful feedback from the participants. Due to the positive feedback received, CSRM will continue to use audience response devices in upcoming sessions. In order to evolve the orientation program further there are some additional improvements planned for 2014. The program will now integrate the content from the ISO manual created by the IS Council into the program so participants have a set of instructions that can be utilized outside of the orientation.

Fifty-one sessions since 2007 have been attended by 469 state agency representatives of independent, judicial and executive branch agencies, including institutions of higher education. The orientation program contributes to a strong commonwealth IT security program. Eighty-eight individuals from 56 agencies attended orientation in 2013. Note: to maintain ISO certifications agencies ISOs only need to attend once every two years.

Information Security Officer Certification

Beginning in 2013, agency ISOs were required to demonstrate a minimum awareness of information security topics. The ISO certification requirements consist of taking courses in the COV Knowledge Center, participating in the IS orientation class, and if desired, maintaining a professional certification in the information security field. CSRM offers all courses necessary to maintain the certification at no cost to the agency. Since 2013 was the first year of the ISO certification program it was not anticipated that all agencies would have a certified ISO. The progress that was made in the first year is commendable, and agency ISOs embraced the opportunity to maintain their knowledge. CSRM also noticed an increase in communication with the ISOs which has also helped immensely. CSRM anticipates that this trend will continue, and that there will be even further improvement next year.

A cornerstone of building an effective IT security program is the agency ISO. The agency's ISO is responsible for maintaining a relationship with the CISO and developing, implementing, and managing the agency's IT security program. Of the 77 agencies, 76 agencies (99 percent) have designated an ISO within the past two years. Of the 76 agencies with ISOs designated, 63 agencies (83 percent) sent primary ISOs to information security orientation; 13 agencies (17 percent) did not have a primary ISO attend within the last two years.


ISO Certifcation Status

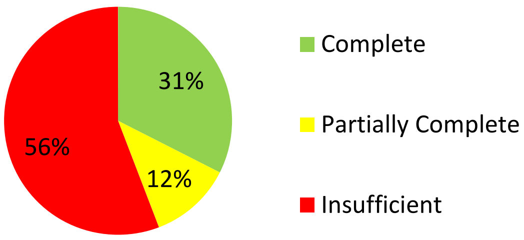
Information Security Audit Program

The Commonwealth's IT security and IT security audit standards require that agencies 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 2013, 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 has been working with agencies to attempt to improve the audit program within the commonwealth; however, there has been little success in improving the scores. Some agencies, such as the Virginia Department of Health, are making excellent progress, but still have at least another year before making adequate improvements. Unless the security audit program improves, CSRM cannot adequately identify areas of weakness within agency environments.

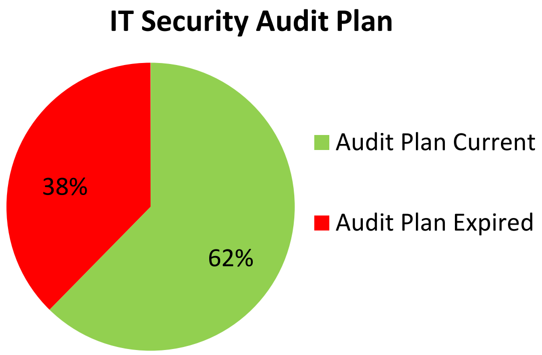
Due to the lack of insight and overall improvement over the last two years CSRM recommends that VITA take additional action to enforce the appropriate security reviews. Some recommended actions include restricting the approval of additional IT projects until agencies with an inadequate audit program establish a viable improvement plan and maintain appropriate improvement against that plan. Additionally, some agencies may require that VITA order security audits on behalf of the agency as described in *2.2-2009*.


Commonwealth Overall Audit Program Score

Commonwealth overall audit program score decreased 1 percent

Submission of a current information security audit plan for sensitive systems - A security audit is an independent review to assess the effectiveness of the controls implemented to safeguard the information stored and/or processed by a system. The Commonwealth uses security audits to determine if the proper controls exist to adequately protect Commonwealth data. The controls of each system are evaluated by the requirements in the Commonwealth Information Security Standard, federal laws, state laws, and regulations. Agency heads must take action to have each sensitive system audited every three years. IT security audit plans provide CSRM with a definitive list of sensitive systems and help the agency schedule the necessary IT security audits of the sensitive systems identified in the risk management process. Each agency head is required to submit the agency IT security audit plan to the CISO annually.

Of the 77 agencies, 48 (62 percent) have submitted a current information security audit plan and 29 (38 percent) have an expired audit plan.

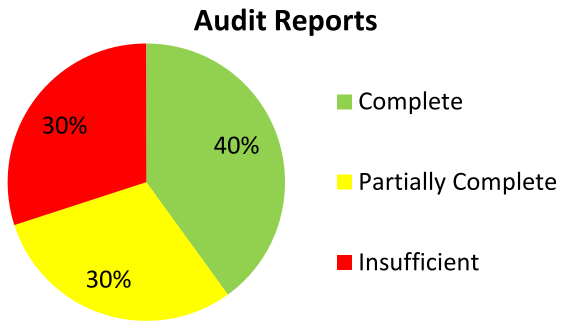


IT security audit plans submitted decreased 9 percent

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

Of the 77 agencies, 30 agencies had sensitive system IT security audits scheduled for 2013. Of those agencies, 12 (40 percent) have submitted all IT security audit reports that are due; nine (30 percent) have submitted some of the IT security audit reports; and nine (30 percent) have not submitted any of the IT security audit reports.

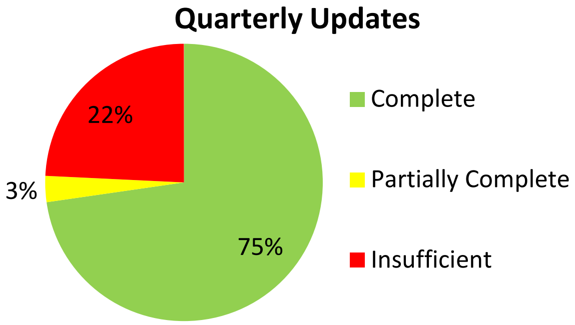
It is important to note that this area shows a decline in the percentage of agencies that have met their anticipated audit schedule. The overall decline is in addition to the fact that fewer audits were scheduled to be completed this year over previous years.



Audit reports submitted decreased 4 percent

Supplied 2013 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 those 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.

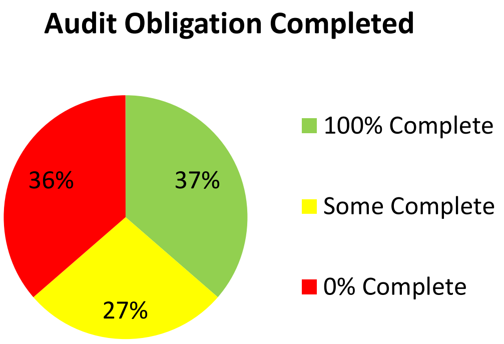
Of the 77 agencies, 32 agencies had quarterly updates due for open corrective action plans in 2013. Of those 32 agencies, 17 (53 percent) have submitted all updates; four agencies (13 percent) have submitted some of the updates; and 11 agencies (34 percent) have not submitted any updates.



Quarterly updates submitted increased 23 percent

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

Of the 77 agencies, 19 (33 percent) have fulfilled completely the obligation to have every sensitive system audited at least once every three years, and 22 (38 percent) have completed partially their audit obligation. At the other end of the spectrum, 17 agencies (29 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.



Three year audit obligations declined 10 percent

Security Audit Findings

One-third of all security audit findings fell into the top two security control families: access control and planning. Ninety-nine percent of all findings were rated high, based on industry standards. Access control was the number one security control family identified by auditors, making up 20 percent of all security audit findings. These findings were typically associated with agency specific applications, and indicate the need for an identity access management standard. A standard would help give guidance in remediating many of these findings.

Access control risk was found to be widespread, with 55 percent of all agencies that submitted audits reporting at least one access control related finding. Access control findings were found to stem from a lack of proper processes for setting up and terminating user roles, groups, privileges, etc., governing access to agency-specific applications. Often all users were granted administrative privileges and were thus able to grant access to other users. This defies the best practice concept of “least privilege,” where each user is only given as much access as needed. Adding to that, many agencies did not have an automated process for removing access when an employee left the agency or moved into a new role that did not require them to have access to that application.

As a result of the widespread use of unnecessarily elevated privileges, unauthorized users could more easily gain access to agency applications. Under these circumstances, a successful phishing attack could grant a malicious actor access to all data within a sensitive system, similar to what occurred in South Carolina where a data breach exposed the Social Security numbers of 3.8 million taxpayers plus credit card and bank account data. That breach is estimated to have cost the state $12 million just to offer citizens one year of third party credit monitoring service. Similarly, the breach at the Target corporation may have been mitigated if tighter access controls had been implemented around the third party vendors that accessed Target’s administrative network. Target claims that the breach exposed approximately 40 million debit and credit card accounts between November 27 and December 15, 2013.

Failure to have a system security plan was the number two finding. The lack of security plans and documentation tie back to the issue of access control. Many agencies need to put together a security plan that includes how they will handle access to their sensitive systems and how those controls impact risk to their business processes and ultimately the commonwealth before bringing those systems online.

Commonwealth Operational Security

Operational cybersecurity includes parts of the information security program that involve addressing and remediating threats and vulnerabilities within agency environments. CSRM collects information from the VITA IT infrastructure program as well as agencies that fall outside the scope of the IT infrastructure program. This information is analyzed on a recurring basis in order to identify threats that are affecting the Commonwealth and identify wide spread vulnerabilities.

It is important to note that there are three agencies that have not yet had enterprise operational controls fully applied due to their status as non-transformed. These agencies remain at a higher level of risk due to the lack of insight into the agency environment and the threats that are impacting them. While there is some limited ability to monitor the environment with partial controls in place agencies will remain at higher risk for intrusion, compromise, and disruption until enterprise controls are applied.

In 2013 CSRM's operational analysis identified three major operational cyber challenges. Two of the issues involved patching of commonly used software and the third included an issue surrounding elevated account privileges. The security operations team leveraged economies of scale to implement enterprise-wide solutions that reduced security incidents within the Commonwealth.

Throughout the Commonwealth there were a total of 73,519 accounts with elevated privileges to employee workstations. This extensive use of elevated privileges posed a significant threat because it could have allowed malicious software to reach COV workstations. CSRM worked with agencies to reduce the number of privileged accounts by 85 percent. As of the end of 2013 there were only 10,922 accounts remaining, with six agencies left to complete. This is a total reduction of 62,597 accounts. The account reduction made it significantly harder for malicious software to run on Commonwealth workstations and helped drive down the number of security incidents for the year.

In addition to CSRM's effort to reduce elevated privileges, there was significant focus on remediating software that no longer received security updates. CSRM's goal was to help agencies either remediate vulnerable software in the environment or put additional security technology in place to protect it from unauthorized access. The two pieces of software that were the focus of this effort were Oracle Java and Microsoft Windows XP.

The first half of 2013 CSRM focused on patching Java instances within the Commonwealth. Initial reviews detected over 35,000 instances within the COV environment, most of which were no longer receiving security patches. After upgrading Java and reducing privileged accounts, CSRM identified a significant reduction in the number of security incidents. Initial results showed a decrease in successful exploits of systems by approximately 57 percent. While the reduction is expected to be temporary as new attack techniques are developed, it was a dramatic drop in security incidents.

The other end of support software issues stemmed from agencies that were unable to migrate off of Microsoft Windows XP. While the Commonwealth has made major strides in upgrading the environment, there are an estimated 5 percent of commonwealth systems that will remain on Windows XP past the end of support date. In order to prevent compromise of the unsupported systems, those systems that must continue running past the support date will have to purchase additional support from Microsoft and, in certain cases, install additional software to further protect the system. It is estimated that the cost to the Commonwealth could exceed $2.2 million. To try and prevent similar situations in the future, CSRM is investigating implementing requirements that agencies address pending end-of-life issues within their environment before new projects and/or IT related purchases occur. The goal is to ensure resources are focused on addressing improving systems that are not cost effective for the Commonwealth to maintain and secure.

Commonwealth Cyber Threat and Attack Analysis

The *Code of Virginia*, *§2.2-603(F)*, requires all executive branch agency directors to report IT security incidents to the CIO within 24 hours of discovery. The Commonwealth Security

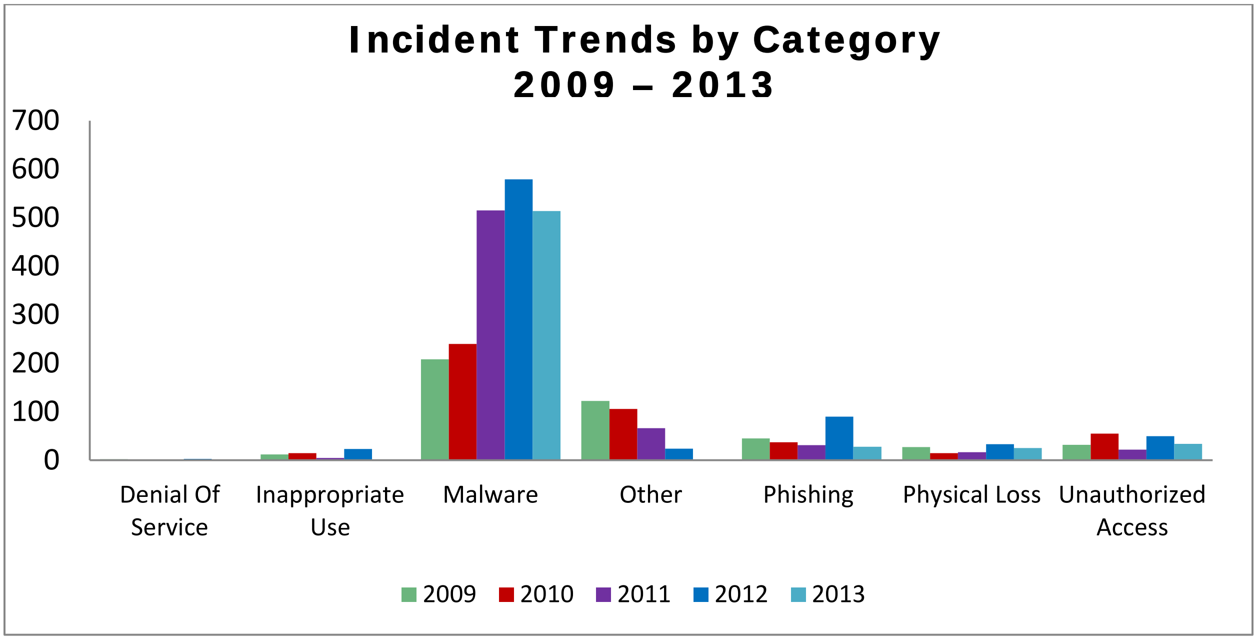
Incident Response Team (CSIRT) categorizes each of these security incidents based on the type of activity.

The data collected in 2013 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 25 percent. In the first half of the year incidents were at a three year high, prompting a coordinated enterprise response. Oracle's Java software was identified as the primary entry point for attackers. In addition, the malicious third parties were leveraging the large number of accounts that had elevated privileges. Once patches were deployed and privileges were reduced, the fourth quarter saw a 57 percent decrease in incidents. 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.

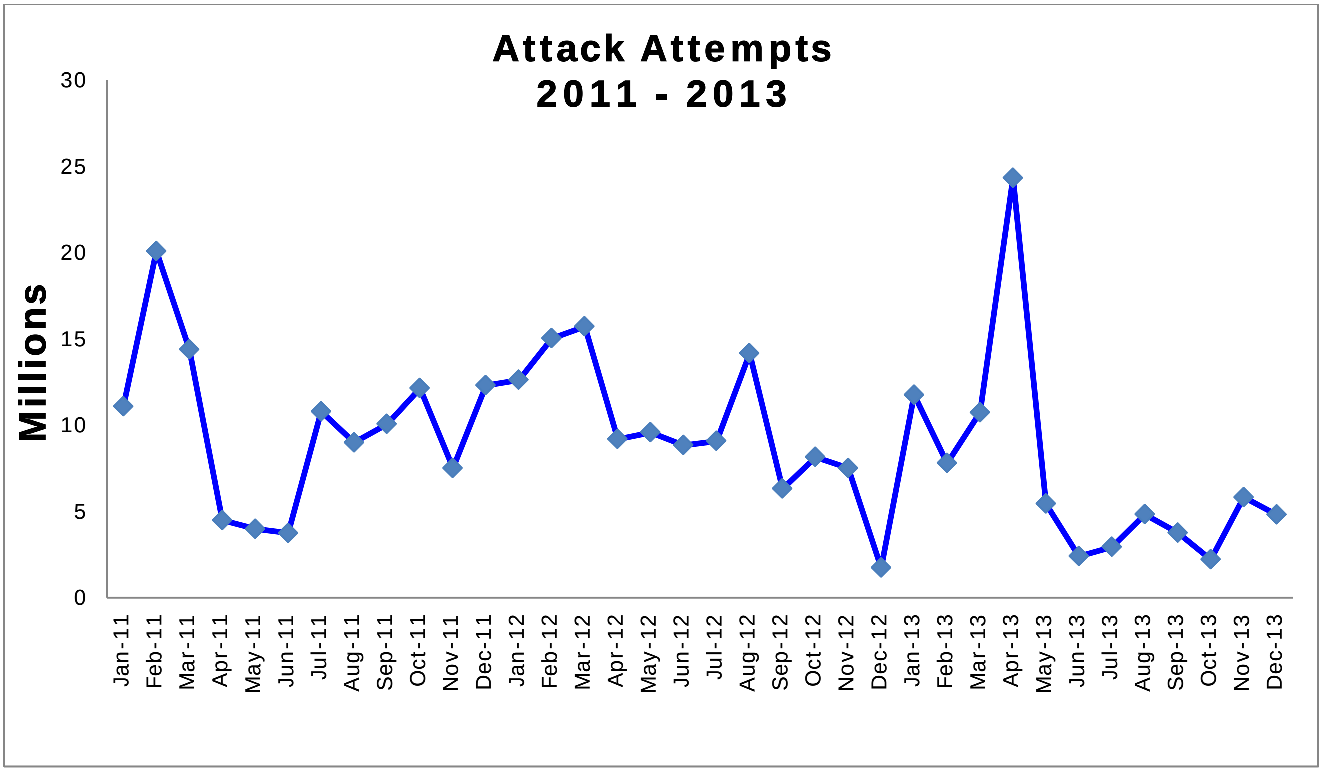
The number of incidents (603) for 2013 still remains a concern. While the initial decrease shows that the coordinated enterprise-wide approach was a success, incident numbers are anticipated to increase as new attack vectors are discovered. In addition there has been an increase of phishing attacks that continue to result in compromised user accounts. In order to reduce the impact of phishing attacks on the Commonwealth, CSRM will begin taking steps to implement two-factor authentication for remote access of systems, where possible. Two-factor authentication will help 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.

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

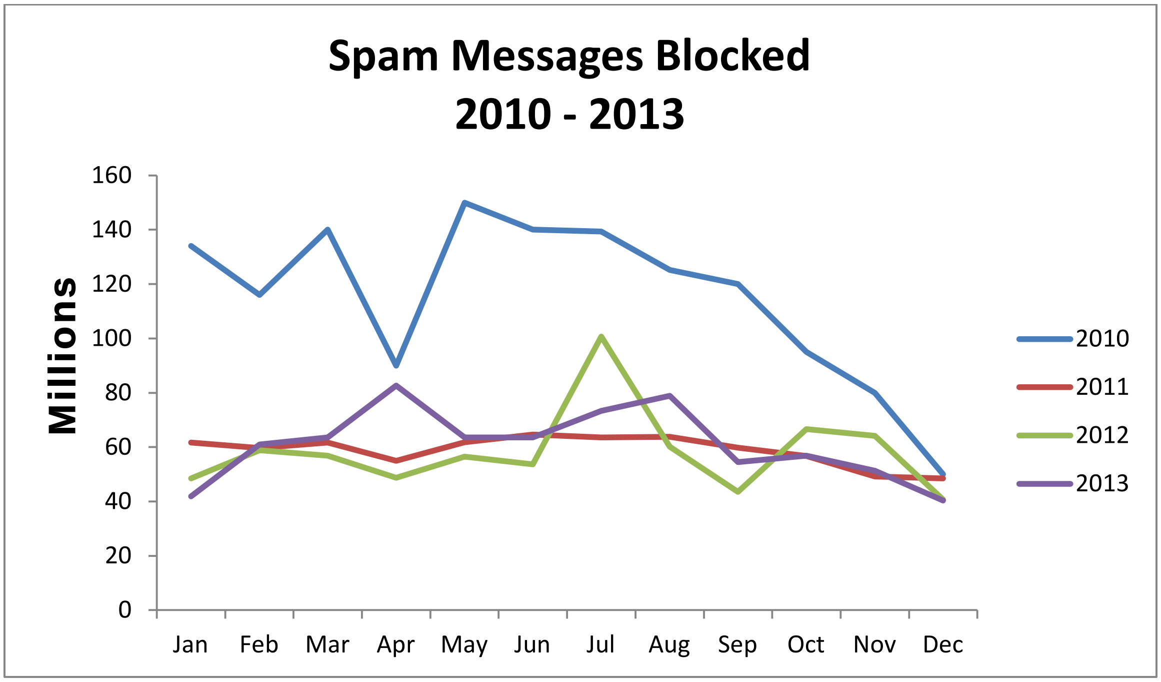
- Denial of service - Loss of availability of a COV service due to malicious activity
- Inappropriate usage - Misuse of COV resources
- Malware - Execution of malicious code such as viruses, spyware and key loggers
- Other - Reports where the investigation determines the event is not a security incident
- 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.)



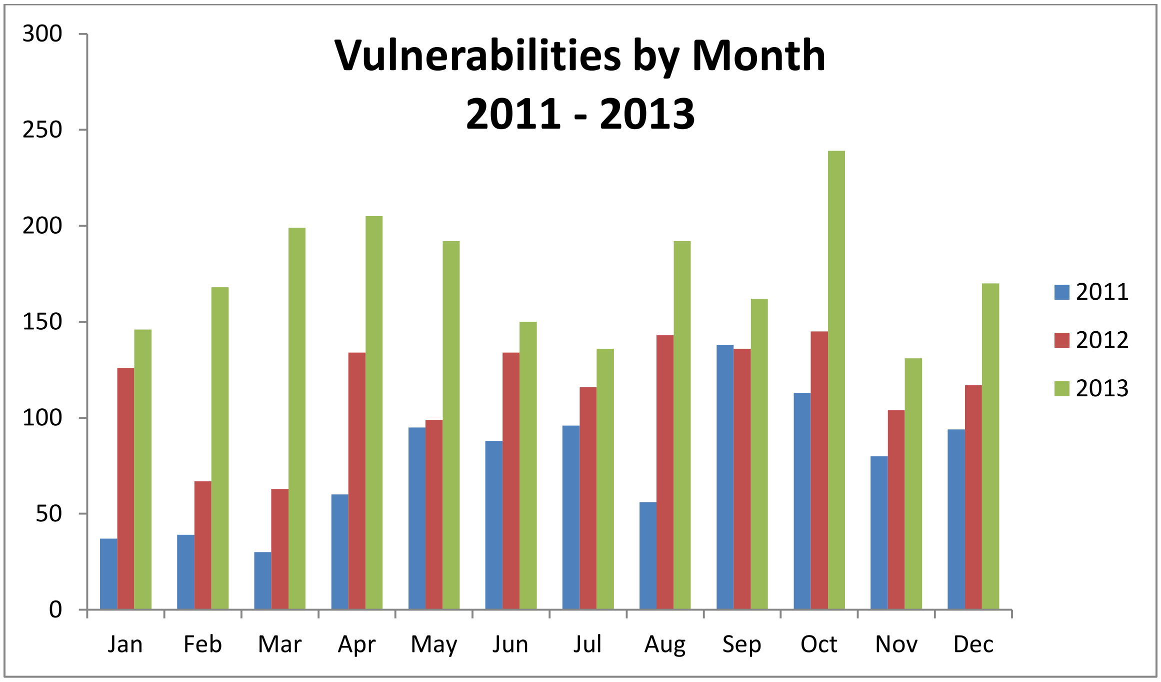
There are additional indicators of the size of the cyber threat to Virginia shown in the data collected from Virginia's primary data center. The Commonwealth received 94,957,601 alerts, or approximately three attacks per second of malicious activity. While the vast majority of attacks were not successful, the number of attack attempts continually challenges Commonwealth IT security personnel to adapt quickly and defend against the constantly shifting cyber threat to prevent data compromise.



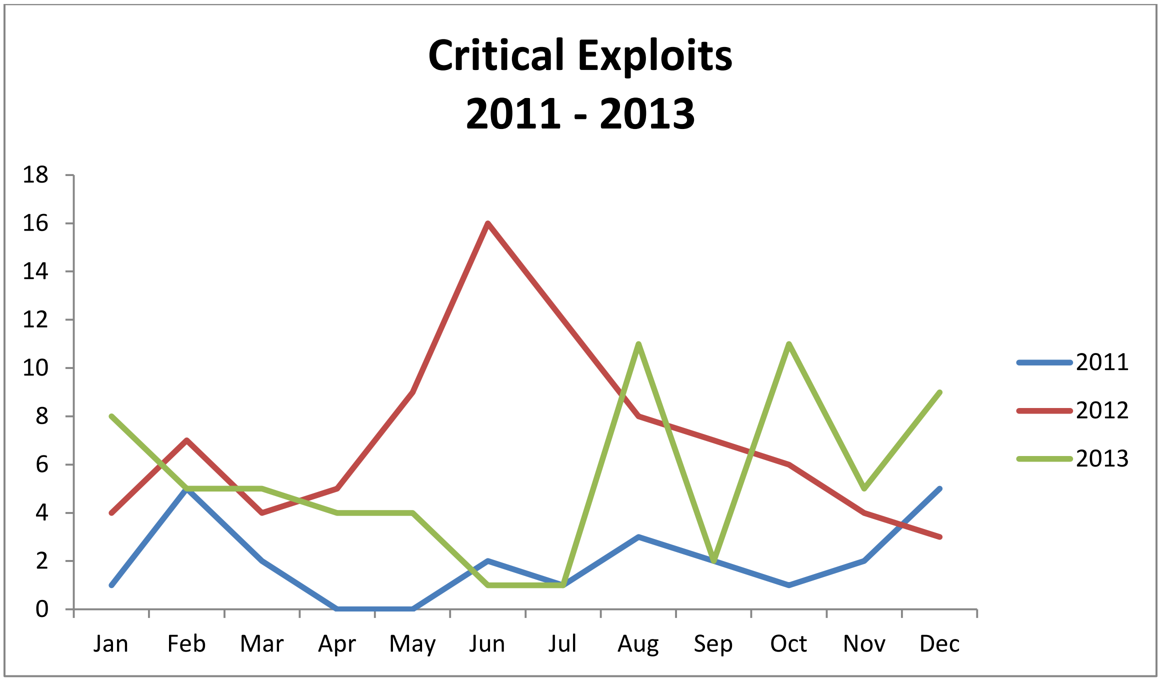
Email is heavily utilized throughout the Commonwealth to carry out daily business. Security tools must be in place because of the heavy usage. Last year, the commonwealth filtered 731,556,544 spam messages and blocked 83,967 viruses from reaching commonwealth assets. Security personnel are constantly fine-tuning the security environment to prevent unsolicited and malicious email from reaching state employees computers. As a result of this protection, users are unaware of how much spam is blocked from their mailboxes.



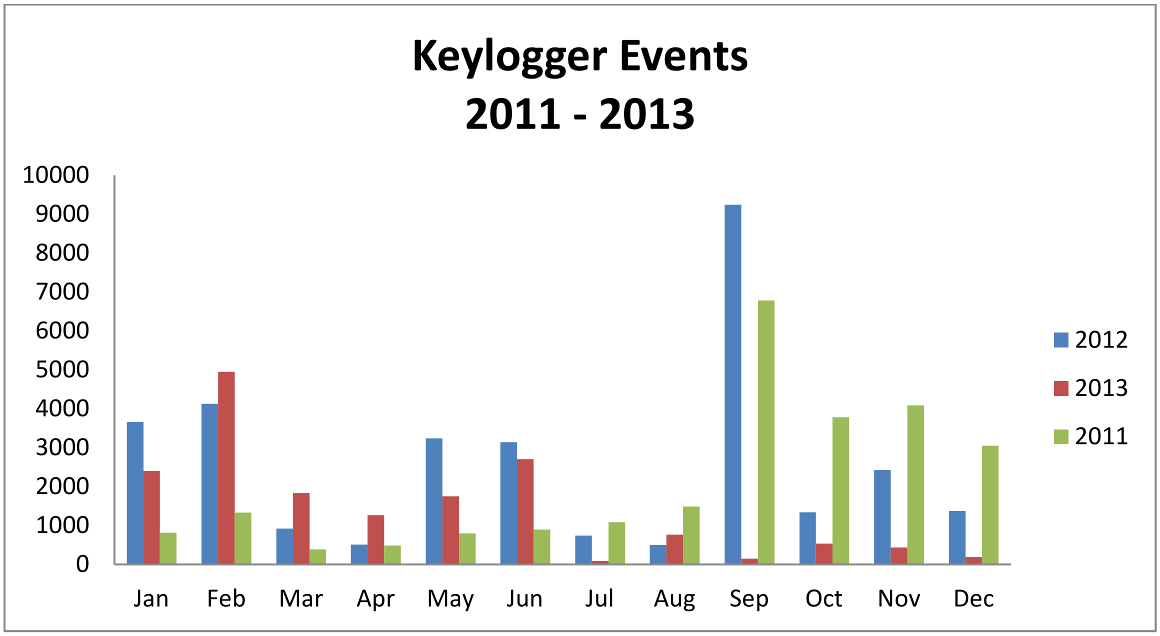
In an effort to foster security awareness, the security incident response team distributes a weekly advisory. This advisory contains information on new vulnerabilities that have been discovered in products that may be in use by state agencies and higher education. During 2013, the number of vulnerabilities being discovered increased each month, with an overall average increase of 150 percent for the year compared to 2012. The increase in vulnerabilities shows the issues that entities have with keeping systems secure.



Of the vulnerabilities that were reported, there was an increase in critical exploits, such as zero day exploits. In 2011, there were 24 critical exploits reported. In 2013, this number rose to 66. This is a 175 percent increase in critical exploits.



The information received from Commonwealth partners includes data involving both state and local governments and citizens. A majority of the data affecting citizens is reported by the Multi-State Information Sharing and Analysis Center (MS-ISAC) as keylogger events. A keylogger event is recorded when CSRM is notified that malicious software designed to record data transactions between the victim and a website or online service belonging to a state or local agency has been used. CSRM works with state agencies to identify the victims of keylogging in order to alert them that their data has been compromised by a malicious third party. In 2013, the Commonwealth experienced 17,037 keylogger events, a 45 percent decrease over 2012. As a result of these events, personally identifiable information for 676 citizens was exposed.



One of the additional services that the cyber security incident response program provides is gathering cyber intelligence information affecting the Commonwealth. While a formal intelligence program is not funded, CSRM provides cyber intelligence information for both agencies and law enforcement within the Commonwealth. CSRM continues to develop relationships with state, federal and local partners. Some of the more notable relationships involve the Virginia Fusion Center, the Virginia State Police, 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 50 state agencies, 39 localities, 22 colleges and universities, and eight public school systems to provide notifications of website defacements, compromised accounts, and malware infections.

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

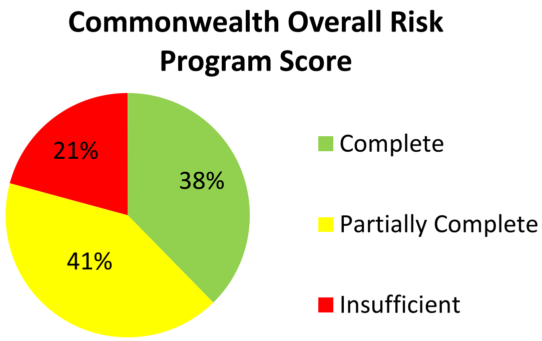
Commonwealth IT Risk Management Program

Commonwealth agencies made improvements in 2013, both in the quantity and quality of BIA, risk assessment, and intrusion detection reporting, most noticeably a 21 percent increase in BIA submissions from the previous year. While the risk management posture has improved since 2012, progress still is needed. CSRM anticipates continued improvement in the risk management program as processes mature.

CSRM started working on a risk management standard in anticipation of the NIST Cybersecurity framework's release in 2014. 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
- 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 risk assessments, business impact analyses and threat data.


Commonwealth Overall Risk Program Score

BIA submissions increased 21 percent

Business Impact Analysis

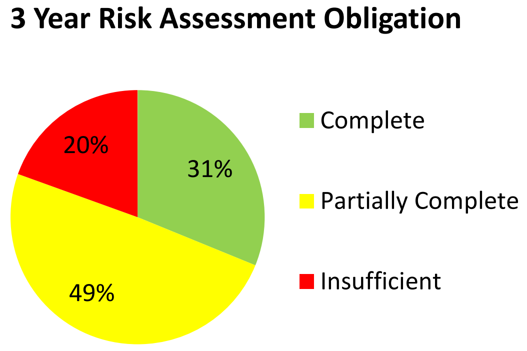
A Business Impact Analysis (BIA) delineates the steps necessary for agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions. Included 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 77 agencies, 60 (78 percent) submitted BIA documentation.

This marked the first year CSRM established a baseline for agency BIAs and analyzed submissions for a specific set of requirements. Of the 60 BIAs submitted, 70 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
- Business functions are rated for impact to life, safety, finance, legal, regulation/compliance, customer service, reputation and citizen privacy
- Mission essential functions were identified
- Recovery time objectives (RTO) were identified

Risk Assessment

A risk assessment is the process of identifying vulnerabilities, threats, likelihood of occurrence and potential loss or impact. Of the 77 agencies, 24 (31 percent) submitted all of the required risk assessment documents. Of the 693 sensitive systems identified, 292 had risk assessments performed.



Risk Assessment Findings

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 with what 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.

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 can then ensure the agencies are prioritizing mitigation of these risks. Agencies that are part of the partnership have their threat metrics reported directly to CSRM on their behalf. Of the 77 agencies, 72 (92 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

The cybersecurity framework will strengthen the Commonwealth's ability to fight cyber crime and further enhance Virginia's position as a leader in cybersecurity. The new framework will help to enhance the systematic process for identifying, assessing, prioritizing and communicating cybersecurity risks; efforts to address risks; and, 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 2013 profile is made up of five functions which are used to group agency data within the framework.

- **Identify**

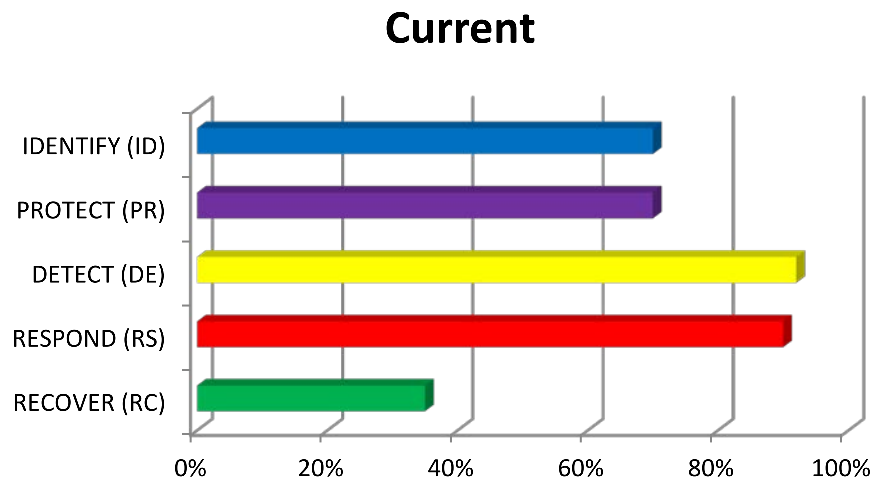
  - Develop the institutional understanding to manage the information security risks to the organizations IT systems, assets, data, and the business functions necessary to accomplish commonwealth agency missions that they support
- **Protect**
  - Develop and implement the appropriate safeguards, prioritized 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	Current	Target
IDENTIFY (ID)	• BIA, RA, IDS, Audit Plan, Quarterly Updates, and Audits submitted averaged 70 percent submission rate, for the commonwealth	• BIA, RA, IDS, Audit Plan, Quarterly Updates, and Audits submitted should be 100 percent
	• Related open findings have been open an average of 420 days	• Asset inventories should be submitted • Related findings should take fewer than 365 days to remediate
PROTECT (PR)	• Related open findings have been open an average of 456 days	• Investigate how to measure effective access controls. • Related findings should take fewer than 365 days to remediate
	• 70 percent of ISOs certified	• 100 percent of ISOs certified
DETECT (DE)	• 92 percent of agencies submitted IDS reports	• 100 percent submission rate for IDS reports
	• Related open findings have been open an average of 444 days	• IDS reporting and or vulnerability scanning results • Related findings should take fewer than 365 days to remediate

RESPOND (RS)	• Each agency should have reported at least one suspected security issue • Related open findings have been open an average of 444 days	• Metrics regarding time to respond to incidents should be benchmarked • Related findings should take fewer than 365 days to remediate
RECOVER (RC)	• 26 of 77 agencies had risk findings regarding issues with their recovery planning • 60 agencies submitted BIAs, 22 with recovery time objectives; 17 percent of agencies submitted audit findings related to recovery planning • Related open findings have been open an average of 444 days	• Related findings should take fewer than 365 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.



Appendix I - Agency Information Security Datapoints - Dashboard

Agency Information Security Datapoints Dashboard - Legend

ISO Designated

🟩 - The agency head has designated an Information Security Officer (ISO) for the agency within the past two years.

🟥 - The agency head has NOT designated an ISO for the agency within the past two years.

Attended ISO Certification

🟩 - The Primary ISO is certified

🟥 - The Primary ISO is NOT certified.

2012 Overall Audit Program

🟩 - Documents received as scheduled

🟨 - Missing CAP(s) or Quarterly update(s)

🟥 - Missing Audit plan

🟥 - Have not met audit obligation

2012 Overall Risk Profile

🟩 - All documentation received as requested information about the agency's BIA, RA(s)[1] , and IDS reports

🟨 - Missing IDS report(s)

🟥 - Missing any required documentation as requested information about the agency's BIA and RA(s)

Agency Information Security Datapoints – Dashboard

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

COV: Agency Data Points

Secretariat	Agency Name	Acronym	ISO Designated	2013 Overall Audit Program	Overall Risk Profile
Public Safety	Alcoholic Beverage Control	ABC	Yes	🟨	🟨
Commerce and Trade	Board of Accountancy	BOA	Yes	🟩	🟩
Technology	Center for Innovative Technologies	IEIA	Yes	🟥	🟥
Public Safety	Commonwealths Attorney's Services Council	CASC	Yes	🟩	🟨
Administration	Compensation Board	CB	Yes	🟥	🟨
Health and Human Resources	Comprehensive Services for At-Risk Youth and Families	CSA	Yes	🟥	🟨
Health and Human Resources	Department for Aging and Rehabilitative Services	DARS	Yes	🟨	🟨
Finance	Department of Accounts	DOA	Yes	🟥	🟨
Transportation	Department of Aviation	DOAV	Yes	🟩	🟩
Health and Human Resources	Department of Behavioral Health and Development Services	DBHDS	Yes	🟥	🟨
Commerce and Trade	Department of Business Assistance	DBA	Yes	🟥	🟥
Natural Resources	Department of Conservation and Recreation	DCR	Yes	🟥	🟥
Public Safety	Department of Corrections	DOC	Yes	🟨	🟩
Public Safety	Department of Criminal Justice Services	DCJS	Yes	🟥	🟨
Education	Department of Education	DOE	Yes	🟥	🟩
Natural Resources	Department of Environmental Quality	DEQ	Yes	🟩	🟩
Public Safety	Department of Fire Programs	DFP	Yes	🟥	🟩
Public Safety	Department of Forensic Science	DFS	Yes	🟩	🟩
Agriculture & Forestry	Department of Forestry	DOF	Yes	🟨	🟩
Natural Resources	Department of Game and Inland Fisheries	DGIF	Yes	🟥	🟨
Administration	Department of General Services	DGS	Yes	🟥	🟨
Health and Human Resources	Department of Health Professions	DHP	Yes	🟥	🟩
Natural Resources	Department of Historic Resources	DHR	Yes	🟩	🟩
Commerce and Trade	Department of Housing and Community Development	DHCD	Yes	🟥	🟨
Administration	Department of Human Resource Management	DHRM	Yes	🟩	🟨
Public Safety	Department of Juvenile Justice	DJJ	Yes	🟨	🟩
Commerce and Trade	Department of Labor and Industry	DOLI	Yes	🟥	🟨
Health and Human Resources	Department of Medical Assistance Services	DMAS	Yes	🟩	🟨
Public Safety	Department of Military Affairs	DMA	Yes	🟥	🟥
Commerce and Trade	Department of Mines, Minerals and Energy	DMME	Yes	🟥	🟨

COV: Agency Data Points

Administration	Department of Minority Business Enterprises	DMBE	Yes	🟥	🟩
Transportation	Department of Motor Vehicles	DMV	Yes	🟥	🟨
Finance	Department of Planning and Budget	DPB	Yes	🟥	🟥
Commerce and Trade	Department of Professional and Occupational Regulation	DPOR	Yes	🟩	🟨
Transportation	Department of Rail and Public Transportation	DRPT	Yes	🟥	🟨
Health and Human Resources	Department of Social Services	DSS	Yes	🟥	🟨
Finance	Department of Taxation	TAX	Yes	🟨	🟨
Finance	Department of Treasury	TD	Yes	🟥	🟩
Public Safety	Department of Veterans Services	DVS	Yes	🟩	🟩
Education	Frontier Culture Museum of Virginia	FCMV	Yes	🟩	🟩
Education	Gunston Hall	GH	Yes	🟥	🟩
Independent	Indigent Defense Commission	IDC	Yes	🟥	🟨
Education	Jamestown-Yorktown Foundation	JYF	Yes	🟥	🟩
Education	Library of Virginia	LVA	Yes	🟩	🟩
Natural Resources	Marine Resources Commission	MRC	Yes	🟩	🟩
Transportation	Motor Vehicle Dealers Board	MVDB	Yes	🟥	🟨
Education	Norfolk State University	NSU	Yes	🟥	🟨
Executive	Office of Attorney General	OAG	Yes	🟥	🟨
Executive	Office of State Inspector General	OSIG	Yes	🟩	🟩
Executive	Office of the Governor	GOV	Yes	🟩	🟨
Education	Richard Bland College	RBC	Yes	🟥	🟨
Education	Science Museum of Virginia	SMV	Yes	🟥	🟥
Education	Southern Virginia Higher Education Center	SVHEC	Yes	🟩	🟥
Administration	State Board of Elections	SBE	Yes	🟥	🟨
Independent	State Corporation Commission	SCC	Yes	🟨	🟥
Education	State Council of Higher Education for Virginia	SCHEV	Yes	🟥	🟨
Independent	State Lottery Department	SLD	Yes	🟥	🟥
Commerce and Trade	Tobacco Indemnification Commission	TIC	Yes	🟥	🟨
Independent	Virginia College Savings Plan	VCSP	Yes	🟩	🟨
Education	Virginia Commission for the Arts	VCA	Yes	🟩	🟩
Agriculture & Forestry	Virginia Department of Agriculture and Consumer Services	VDACS	Yes	🟩	🟩
Public Safety	Virginia Department of Emergency Management	VDEM	Yes	🟥	🟩

COV: Agency Data Points

Health and Human Resources	Virginia Department of Health	VDH	Yes	🟨	🟨
Transportation	Virginia Department of Transportation	VDOT	Yes	🟩	🟩
Commerce and Trade	Virginia Economic Development Partnership	VEDP	Yes	🟥	🟥
Commerce and Trade	Virginia Employment Commission	VEC	Yes	🟩	🟨
Health and Human Resources	Virginia Foundation for Healthy Youth	VFHY	Yes	🟥	🟥
Technology	Virginia Information Technologies Agency	VITA	Yes	🟥	🟩
Education	Virginia Museum of Fine Arts	VMFA	Yes	🟥	🟥
Natural Resources	Virginia Museum of Natural History	VMNH	Yes	🟥	🟥
Commerce and Trade	Virginia Racing Commission	VRC	Yes	🟩	🟩
Commerce and Trade	Virginia Resources Authority	VRA	No	🟥	🟥
Independent	Virginia Retirement System	VRS	Yes	🟩	🟩
Education	Virginia School for the Deaf and Blind	VSDB	Yes	🟥	🟥
Public Safety	Virginia State Police	VSP	Yes	🟩	🟩
Education	Virginia State University	VSU	Yes	🟨	🟩
Independent	Virginia Workers Compensation Commission	VWC	Yes	🟩	🟩

Appendix II - Agency Information Security Datapoints - Dashboard

Agency Information Security Datapoints Dashboard - Legend

Attended IS Orientation, KC Training and ISOAG Meetings

🟢 - The primary ISO is certified

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

🔴 - The primary ISO is NOT certified

2013 Audit Plan Status

🟢 - Documents received as scheduled

🔴 - Missing audit plan

2013 Business Impact Analysis Status

🟢 - All documentation received as requested

🟡 - Documentation received, but incomplete

🔴 - 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 Acronym	ISO Certification Status	Audit Plan Status	Percentage of Audits Received	Percentage of Quarterly Updates Received	3 Year Audit Obligation	Business Impact Analysis Status	3 Year Risk Assessment Obligation
Agency Secretariat: Administration							
CB	🟢	🔴	0%	N/A	0%	🟡	0%
DGS	🟢	🟢	100%	100%	33%	🟡	0%
DHRM	🟢	🟢	N/A	N/A	100%	🟡	0%
DMBE	🔴	🔴	N/A	N/A	100%	🟡	100%
SBE	🟢	🔴	N/C	N/A	N/C	🟢	0%
Agency Secretariat: Agriculture & Forestry							
DOF	🟢	🟢	N/A	75%	100%	🟢	100%
VDACS	🟢	🟢	100%	100%	100%	🟢	90%
Agency Secretariat: Commerce and Trade							
BOA	🟢	🟢	N/A	N/A	100%	🟢	100%
DBA	🟡	🔴	N/C	N/A	N/C	🔴	N/C
DHCD	🔴	🟢	N/A	0%	40%	🟢	0%
DOLI	🔴	🔴	N/C	N/A	N/C	🟡	N/C
DMME	🟢	🔴	0%	0%	20%	🟡	0%
DPOR	🔴	🟢	80%	N/A	100%	🟡	60%
TIC	🟡	🟢	N/A	N/A	0%	🟢	0%
VEDP	🟡	🟢	N/A	N/A	0%	🔴	0%
VEC	🟢	🟢	100%	100%	100%	🟡	3%
VRC	🟢	🟢	N/A	N/A	N/A	🟢	100%
VRA	N/C	🔴	N/C	N/A	N/C	🔴	N/C
Agency Secretariat: Education							
DOE	🟢	🟢	N/A	100%	44%	🟢	90%
FCMV	🔴	🟢	N/A	N/A	N/A	🟢	N/A
GH	🔴	🔴	N/C	N/A	N/C	🔴	0%

COV: Agency Data Points

Agency Acronym	ISO Certification Status	Audit Plan Status	Percentage of Audits Received	Percentage of Quarterly Updates Received	3 Year Audit Obligation	Business Impact Analysis Status	3 Year Risk Assessment Obligation
JYF	🟢	🟢	N/A	N/A	17%	🟢	83%
LVA	🔴	🟢	N/A	N/A	100%	🟢	100%
NSU	🟢	🔴	0%	N/A	13%	🟢	0%
RBC	🟡	🔴	N/A	N/A	0%	🟢	40%
SMV	🔴	🔴	N/A	N/A	0%	🔴	0%
SVHEC	🔴	🟢	N/A	N/A	N/A	🔴	N/A
SCHEV	🔴	🟢	N/A	N/A	0%	🟢	0%
VCA	🔴	🟢	N/A	N/A	N/A	🟢	N/A
VMFA	🔴	🔴	N/A	0%	0%	🔴	0%
VSDB	🟢	🔴	N/A	N/A	0%	🔴	0%
VSU	🟢	🟢	100%	100%	81%	🟢	100%
Agency Secretariat: Executive							
OAG	🔴	🔴	N/A	N/A	67%	🟡	0%
OSIG	🟢	🟢	N/A	N/A	N/A	🟢	N/A
GOV	🔴	🟢	N/A	N/A	N/A	🔴	N/A
Agency Secretariat: Finance							
DOA	🟢	🔴	N/A	0%	53%	🟡	0%
DPB	🔴	🔴	N/C	0%	N/C	🔴	N/C
TAX	🟢	🟢	100%	100%	69%	🟡	58%
TD	🟢	🟢	N/A	N/A	0%	🟢	100%
Agency Secretariat: Health and Human Resources							
CSA	🟢	🔴	N/A	N/A	0%	🟢	0%
DARS	🟢	🟢	100%	100%	64%	🟡	0%
DBHDS	🟢	🔴	N/C	N/A	N/C	🔴	55%
DHP	🟢	🟢	N/A	N/A	50%	🟢	100%

COV: Agency Data Points

Agency Acronym	ISO Certification Status	Audit Plan Status	Percentage of Audits Received	Percentage of Quarterly Updates Received	3 Year Audit Obligation	Business Impact Analysis Status	3 Year Risk Assessment Obligation
DMAS	🟢	🟢	98%	100%	100%	🟡	40%
DSS	🔴	🟢	N/A	0%	25%	🟢	0%
VDH	🟢	🟢	100%	100%	67%	🟢	0%
VFHY	🔴	🔴	N/C	N/A	N/C	🔴	N/C
Agency Secretariat: Independent							
IDC	🟢	🟢	50%	100%	33%	🟢	0%
SCC	🟡	🟢	100%	100%	100%	🟡	0%
SLD	🟢	🔴	0%	0%	0%	🔴	0%
VCSP	🟢	🟢	100%	N/A	100%	🟢	100%
VRS	🟢	🟢	100%	100%	100%	🟡	90%
VWC	🟢	🟢	100%	100%	100%	🟢	100%
Agency Secretariat: Natural Resources							
DCR	🟢	🔴	0%	0%	33%	🔴	0%
DEQ	🟢	🟢	100%	100%	100%	🟢	100%
DGIF	🔴	🟢	N/A	N/A	52%	🟢	0%
DHR	🟢	🟢	N/A	100%	N/A	🟢	N/A
MRC	🟢	🟢	N/A	N/A	100%	🟢	100%
VMNH	🔴	🔴	N/C	N/A	N/C	🔴	N/C
Agency Secretariat: Public Safety							
ABC	🟢	🟢	100%	100%	72%	🟢	20%
CASC	🔴	🟢	N/A	N/A	N/A	🔴	N/A
DOC	🟢	🟢	100%	100%	92%	🟢	100%
DCJS	🟡	🔴	N/C	N/A	N/C	🟡	N/C
DFP	🟢	🟢	0%	N/A	0%	🟢	100%

COV: Agency Data Points

Agency Acronym	ISO Certification Status	Audit Plan Status	Percentage of Audits Received	Percentage of Quarterly Updates Received	3 Year Audit Obligation	Business Impact Analysis Status	3 Year Risk Assessment Obligation
DFS	🟢	🟢	N/A	100%	100%	🟢	100%
DJJ	🟢	🟢	50%	100%	100%	🟢	100%
DMA	🔴	🔴	N/C	N/A	N/C	🔴	N/C
DVS	🟢	🟢	N/A	N/A	100%	🟢	100%
VDEM	🟢	🟢	0%	N/A	0%	🟢	83%
VSP	🟢	🟢	100%	100%	100%	🟢	92%
Agency Secretariat: Technology							
IEIA	🟢	🔴	N/C	N/A	N/C	🟢	N/C
VITA	🟢	🟢	0%	100%	0%	🟢	88%
Agency Secretariat: Transportation							
DOAV	🟡	🟢	N/A	100%	100%	🟢	100%
DMV	🟢	🔴	7%	100%	93%	🟡	0%
DRPT	🔴	🔴	N/C	N/A	N/C	🟢	N/C
MVDB	🔴	🔴	N/C	N/A	N/C	🟢	N/C
VDOT	🔴	🟢	100%	100%	100%	🟡	89%