

Virginia Information Technologies Agency



2016 Commonwealth of Virginia Information Security Report



www.vita.virginia.gov

Prepared and Published by:
Virginia Information Technologies Agency
VITA - Powering the commowearth's digital government

Comments on the
2016 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



Contents

Commonwealth Threat Management Program	8
Commonwealth Cyber Threat and Attack Analysis	9
Cyber security incident trends continue to be monitored.	10
Incident Trends by Category	12
SPAM Messages	13
CSRM Security Services Center	17
IT Security Audit Services	17
ISO Services	17
Vulnerability Scanning Services	18
Commonwealth Information Security Governance Program	19
Statute Requires Compliance Monitoring	19
Key Commonwealth Security Audit Compliance Metrics and Analysis	19
Commonwealth Information Security Officers Advisory Group.....	22
Cybersecurity Strategy Development and Monitoring.....	23
Commonwealth Information Security (IS) Council	24
Compliance Report Card	24
Commonwealth IT Risk Management Program	25
IT Risk Management Program Monitoring	25
Cybersecurity Framework Assessment	28
Appendix I - Agency Information Security Data Points - Dashboard.....	30
Appendix II - Agency Information Security Data Points - Detail.....	35
Appendix III – Cybersecurity Framework Results - Detail	40



This 2016 Commonwealth of Virginia (COV) Information Security Report is the ninth 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 Level I institutions of higher education. This report does not address compliance for Level II and Level III 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. 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 security compliance metrics is found in the appendices of this document.

The commonwealth increased IT security funding to support agency information security programs. Agencies were allocated more than \$15 million in the FY2017 and FY2018 biennial budget to strengthen their IT security programs. The funding was established to address the high percentage of agencies that were not able to adequately implement their information security programs. The results from the funding should start to show an upward trend in the number of agencies with adequate information security programs over the coming years.

VITA established additional centralized services to support agency information security programs. VITA began offering security IT audit services and information security officer (ISO) services as an additional information security resource for the commonwealth. These services are intended to help agencies evaluate their IT security programs and comply with commonwealth IT security audit requirements. There were 25 agencies that elected to use the VITA IT audit service to enhance their IT security audit programs and 26 agencies that participated in the ISO program. In addition, CSRM performed more than 1,300 vulnerability scans of public-facing websites in 2016 to begin the mandated vulnerability scanning program. Vulnerability scans identify potential security weaknesses that could be exploited to gain access to sensitive commonwealth information. Agencies began using the results of the scans to develop corrective action plans to address these weaknesses and further safeguard agency information. With additional funding, IT security audits, enhanced risk assessment programs, and vulnerability scans, the commonwealth is better positioned to safeguard its information assets.



Security awareness education will continue to be a priority to combat the increasing social engineering threats and malware attacks directed at the commonwealth. Social engineering, a deceitful tactic to get someone to reveal sensitive information, was the leading cause of information security incidents in the commonwealth. The second leading cause of incidents was malware -- malicious software that appears to be legitimate but is intended to damage computer systems or gain unauthorized access to sensitive records. To supplement long established requirements for agencies to conduct security awareness training for their employees and contractors, VITA conducts phishing campaigns to test awareness and determine if users recognize social engineering attempts and emails that might contain malware. CSRM recommends that agencies promote wise and responsible use of commonwealth information by establishing a culture of control, providing guidance on appropriate use, effective training, and holding employees accountable for improper use of sensitive records.

VITA established new third party hosting (also known as cloud hosting) IT security standards. While several IT standards were updated in 2016, the Hosted Environment Information Security Standard was a key standard that was implemented to establish the baseline for information security and risk management activities associated with commonwealth data stored in a non-commonwealth location. The successful implementation of this standard is a critical part of the commonwealth's third party hosting strategy to ensure that commonwealth data is stored in a secure environment with protections appropriate to the sensitivity of the information.

Agency audit program compliance increased slightly. Agency three year audit obligations and the current year of completed audits declined; however, the completion of audit plans and quarterly updates submitted increased, which resulted in a slight increase in audit program compliance. IT security audits play a critical role in providing assurance that IT security controls in the commonwealth are designed and operating effectively to safeguard commonwealth information. When audits are not completed in a timely manner, these controls and potential weaknesses may not be adequately identified and addressed. As agencies begin to utilize IT security funds allocated to develop their IT security programs, including utilizing the VITA IT security audit services offered, CSRM anticipates that IT security audit compliance metrics will improve.

CSRM participated in VITA IT procurement efforts to advocate for IT security requirements as a part of the IT infrastructure sourcing process. As VITA continues to work toward a multi-supplier service platform, CSRM actively participated in developing requirements, reviewing proposals, and assessing security requirements for a myriad of potential IT vendors. Furthermore, CSRM, along with personnel from the Department of Motor Vehicles (DMV), Department of Forestry (DOF), Department of Taxation (TAX), Department of Juvenile Justice (DJJ), Department of Aging and Rehabilitative Services (DARS), Department of Education (DOE), Department of Accounts (DOA), and Virginia College Savings Plan (VCSP), worked toward procuring IT security services for the commonwealth. These combined efforts were designed so that security



services offered will meet commonwealth security requirements and satisfy the wants and needs of the agencies.

A work group should be convened to study cybersecurity threats facing higher education and develop an action plan to combat these threats. Institutions of higher education are frequently targeted by cyber attackers to obtain the sensitive information they manage, such as personal health records, intellectual property and financial information. These records are attractive to malicious hackers who want to misuse this information, as evidenced by Multi-State Information Sharing and Analysis Center (MS-ISAC) records that show that higher education now leads other public entities in the number for security investigations for accounts compromised, malware infections, cyberattacks and software vulnerabilities. In the Commonwealth of Virginia, Level II and Level III institutions may be allowed operational authority over their IT programs. If granted, these institutions are not subject to external IT security governance, which could assist these institutions by providing consistent IT policies and standards, monitoring compliance with established requirements, and facilitating incident management and response. To address these issues, CSRSM recommends that that commonwealth convene a work group to study the current IT governance structure for higher education and develop recommendations to address the persistent security threats facing these institutions.

Agency risk management programs need improvement to identify information security risks in agency environments. Risk program compliance is low, with only 40 percent of agencies having implemented comprehensive risk management programs. This is an increase of 5 percent from the prior year; however, more than half of the agencies did not have approved risk assessment plans, risk assessments and/or business impact analysis. These tools are critical to demonstrate that the agencies have adequately assessed the potential threats and vulnerabilities to agency IT systems and their environments and the likelihood that threats will materialize. The business impact analysis identifies 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. These are important tools for allocating resources and continuity planning. CSRSM recommends that agencies redouble their efforts to develop their risk management programs. As agencies begin to utilize IT security funds allocated to develop their IT security programs, including VITA ISO services, CSRSM anticipates that risk management program compliance metrics will increase.

Information security is an integral part of the IT strategic planning process to confirm that security needs are considered as a part of the agency's overall strategic planning process. CSRSM considers the adequacy of an agency's information security program when reviewing its strategic plans to determine if agency resources have been allocated to resolve existing security issues prior to investing in new technologies. These compliance metrics indicate if there are existing security issues that should be resolved before the agency invests in new technology. CSRSM recommends that agencies resolve outstanding operational risks/issues (ORIs), such as end-of-life systems, promptly



to enhance overall agency security and expedite the CSRM review of the agencies' strategic plans.

Most agencies participated in the National Cyber Security Review (NCSR), a self-assessment survey based on National Institute of Standards and Technology (NIST) cybersecurity framework. Agencies were tasked with participation in the NCSR to evaluate their cybersecurity processes and posture in comparison to security best practices and contribute to the nation's cyber risk assessment process. Overall, 69 percent of agencies participated in the survey. The results were summarized by the core elements of the NIST cybersecurity framework, which are the following basic cybersecurity functions: identify, protect, detect, respond and recover. Survey results indicated that agencies on average have partially documented standards and/or procedures in all five cybersecurity functions. Agencies reported that their processes were least mature in the "recover" function, where agencies need to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity event. The "protect" function, related to agencies' ability to limit or contain the impact of a potential cybersecurity event, is where agencies indicated their processes were the most mature. Agencies should use the survey results to prioritize their efforts to develop security controls where needed to reduce risk. In addition, agencies can use the results as a benchmark to gauge progress in the maturity of their cybersecurity posture and assist in cybersecurity investment decisions. Agencies should strive toward optimized maturity where each organization has policies, standards and/or procedures to achieve their objectives, and implementation is not only tested and verified but also regularly reviewed, improved and repeated to ensure continued effectiveness of their controls.



The 2016 Annual Security Report for the Commonwealth of Virginia report includes an analysis of the commonwealth threat management program, new services offered, the commonwealth information security governance program and the commonwealth risk management program.

Commonwealth Threat Management Program

The threat management program is designed to monitor and manage potential malicious IT attacks against commonwealth agencies and information. To assess the commonwealth's overall threat posture, CSRМ 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. Some of the key components of the program are highlighted in this report.

The commonwealth security incident response team (CSIRT) continues to develop cyber incident response playbooks. These playbooks will facilitate incident response by providing detailed, written guidance for identifying, containing, repairing and recovering from an incident. The playbooks will consider incident response in a multi-supplier service platform environment and the unique requirements of that environment. The playbooks will promote incident response preparedness, consistency and overall effectiveness.

State agencies that have not been transformed, but participate in the commonwealth's IT infrastructure, face growing information security risks. The Virginia Department of Emergency Management (VDEM) and Virginia Employment Commission (VEC) are making plans to transition to the IT infrastructure offerings replacing the Comprehensive Infrastructure Services Agreement (CIA) for IT infrastructure services that expires July 1, 2019. The new offerings will provide these agencies with all of the benefits of transformation under the previous model, including added security and improved incident response processes.

In contrast, Virginia State Police (VSP) rejected transformation efforts and provides their own computer infrastructure in support of their public safety mission. In 2016, VSP proposed an enterprise-wide solution for their agency that would include additional staffing, hardware and software, independent of VITA. However, the corresponding costs for the proposal were too high and the VSP request was not supported by the legislature. VSP continues to refuse to transform their environment and as a result, VSP's hardware and software remains without the security controls that have been implemented in the rest of the enterprise environment. This increases the risk to VSP's environment and leaves them vulnerable to attacks that would otherwise be mitigated by enterprise tools, such as monitoring and intrusion detection. These risks are increasing as software continues to reach end-of-life and support expires. CSRМ recommends that VSP plan to participate in the enterprise service offerings to ensure adequate enterprise security controls are established to protect their sensitive records.



CSRM is implementing the next generation of security services to support the enterprise environment and provide options for non-enterprise entities. CSRM has been leading efforts to procure new IT security solutions and plan for transition from the commonwealth's current sourcing partner. CSRM is working with personnel from DMV, DOF, TAX, DJJ, DARS, DOE, DOA, and VCSP to create, review, and evaluate request for proposal (RFP) documents to procure IT security services for the commonwealth. VITA and agency personnel worked together to create a model which ensures security services offered will protect the commonwealth from cyber threats as well as satisfy agency wants and needs. In addition, CSRM has been involved in the overall IT sourcing effort at VITA including the disentanglement process to ensure that controls are in place to protect the confidentiality, integrity and availability of commonwealth information assets.

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 in accordance with security standard SEC501-09. The CSIRT then categorizes each security incident based on the type of activity.

During 2016, the Commonwealth of Virginia continued to be a target for cyberattack. The commonwealth experienced 86 million attack attempts on the network and blocked 832 million pieces of spam and more than 144,000 pieces of malware. Despite many layers of protection, the commonwealth still experienced 320 successful IT security incidents. While this is a 14 percent decrease from 2015, the most vulnerable aspect of our systems is still the user.

Social engineering remains the number one risk to commonwealth systems.

Social engineering, a deceitful tactic used by attackers to get a system user to reveal sensitive information, was used against state employees to allow unauthorized remote access to systems and to provide credentials to unknown entities. These types of attacks constituted 139 of the 320 (43 percent) of the incidents for the year. Of the 139 incidents, 93 (67 percent) resulted in compromised credentials being used by the attacker.

While social engineering attacks were a large threat from users, they were not the only threat that users posed to the commonwealth's data and IT systems. Of the 320 incidents that occurred, 29 percent were attributed to malware and other types of cyberattacks. Forty-nine incidents (15 percent) were the result of users losing or having state assets stolen. Thirty-four incidents (11 percent) resulted from data being disclosed to unauthorized users and five incidents were a result of inappropriate use of state equipment.

In order to evaluate IT security awareness with state employees, CSRM conducted a state-wide simulated phishing campaign. The campaign covered 40,892 employees across 91 state agencies, which included some non-executive branch agencies. Of the simulated phishing messages that were sent, 21,617 (53 percent) employees opened the message. Of those employees who opened the emails, 5,384 employees (25 percent) clicked on the link inside the email and 3,384 employees who clicked the link submitted their credentials.



This was 63 percent of the users that clicked on the link. As the incident totals for 2016 indicate that 67 percent of users responding to a phishing campaign had their compromised credentials used by the attacker, the simulated campaign results were in line with the actual results for 2016.

In order to reduce the number of incidents, CSRSM has been working with agencies to encourage user training to improve the ability for users to identify social engineering attacks. Additionally, CSRSM has designed security controls which reduce the effectiveness of phishing in the upcoming messaging services of the IT infrastructure program. In the meantime, the incident response team has continued to offer simulated phishing campaigns to agencies. During the second half of 2016, CSRSM performed simulated phishing campaigns at four agencies as part of their security awareness training programs. These simulated phishing campaigns were developed on an individual basis for each agency to be relevant to that agency's business needs. Campaigns were run for several days and detailed reports were provided to agency ISOs at the end of the campaign. This training exercise assists an agency's ISO in evaluating the level of security awareness training that is needed for the agency.

Malware remains a serious threat to commonwealth systems.

The second largest category of incidents for 2016 was malware. Malware programs are designed to infect legitimate users' computers to damage systems or provide unauthorized access to sensitive records. Of the 83 malware incidents experienced in 2016, the two most prevalent categories were Trojans, with 40 reported incidents and ransomware with 34 reported incidents. The remainder of malware incidents were scattered across various categories. Trojan malware pretends to be legitimate software to entice the end user to run it. It also can be hidden in email attachments and run automatically. Trojans are known for establishing backdoors on systems or exploiting vulnerabilities to gain access to the user's system, allowing data to be stolen. Ransomware, malware that is used to extort money from the user by restricting access to the user's data until they pay the ransom, can be contracted through visiting a website or opening an email attachment. Once the ransomware is installed, it conducts a handshake with its command and control server to download the key used to encrypt the data. Many times the key that is received after the ransom is paid fails to decrypt the data, so the user still cannot gain access to their information. Therefore, the best option for re-gaining access to the data is to restore the data from a clean backup.

CSRSM is using best practices to combat malware. Some of the best practices being employed include: keeping anti-virus software up to date, installing host intrusion detection software on devices, working with agencies to restrict local administrator rights and publishing a weekly security advisory.

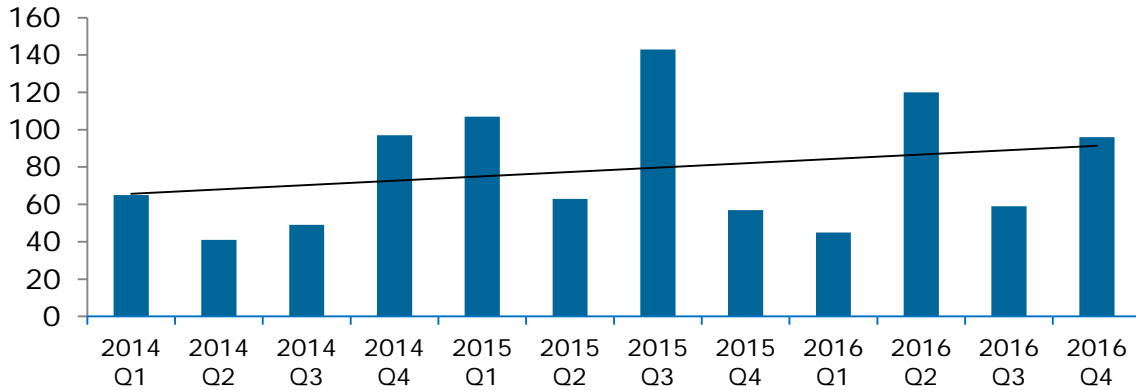
Cyber security incident trends continue to be monitored.

Over the past five years, CSRSM has been working diligently to protect commonwealth systems from cyber threats. As best practices are implemented and additional layers of protection are added, attackers develop new tactics to compromise systems. CSRSM is

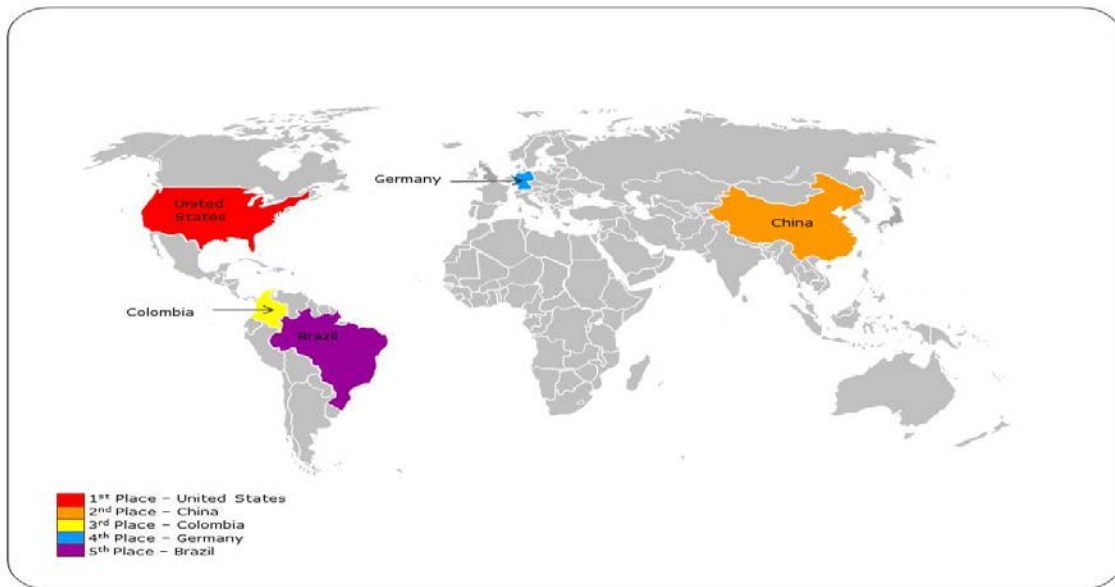


continually investigating new security controls to protect the environment from compromise.

Incident Trends 2014 – 2016



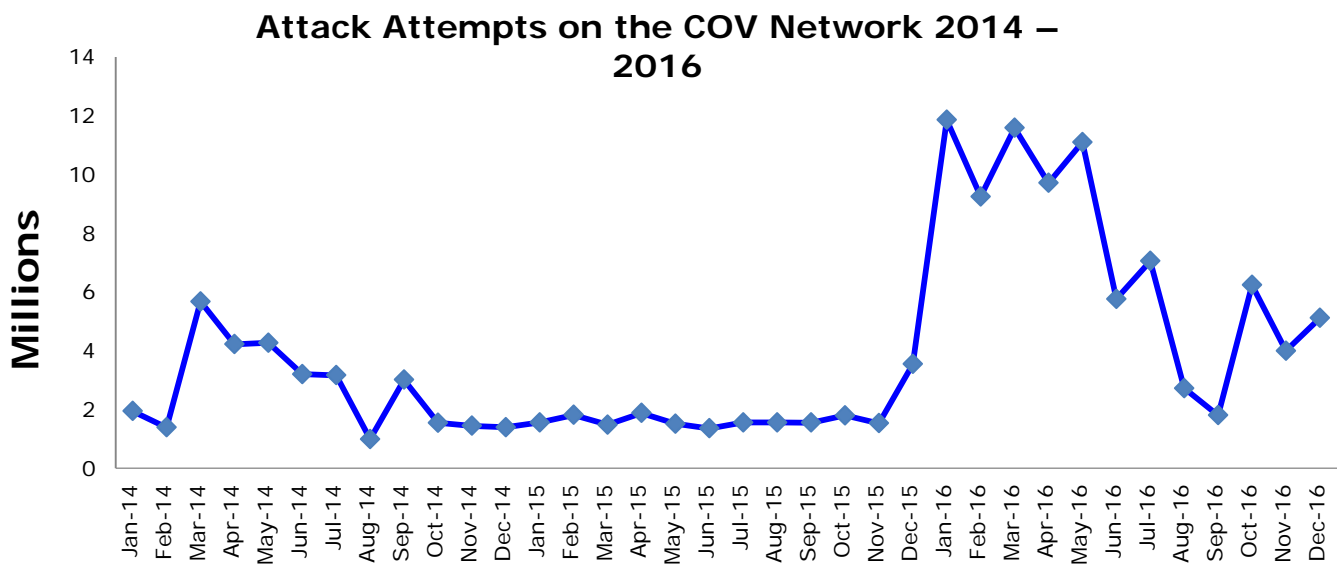
The origins of the attacks on the commonwealth’s network are monitored and tracked. While attackers often try to obscure their locations, this analysis indicated that the top five countries where attacks originated were the United States, China, Colombia, Germany and Brazil. This reveals the increasingly 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.





Attack Attempts

During 2016, over 86 million attack attempts were detected against commonwealth systems. This is a rate of one attack every 2.73 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. For the first three quarters of 2016, the commonwealth experienced a significant increase in the number of domain name system (DNS) reply sinkhole attacks. This type of attack occurs when a sinkhole, a standard DNS server that is configured to protect the network, replies to any DNS request that goes out to ad servers and blocks the traffic.



Incident Trends by Category

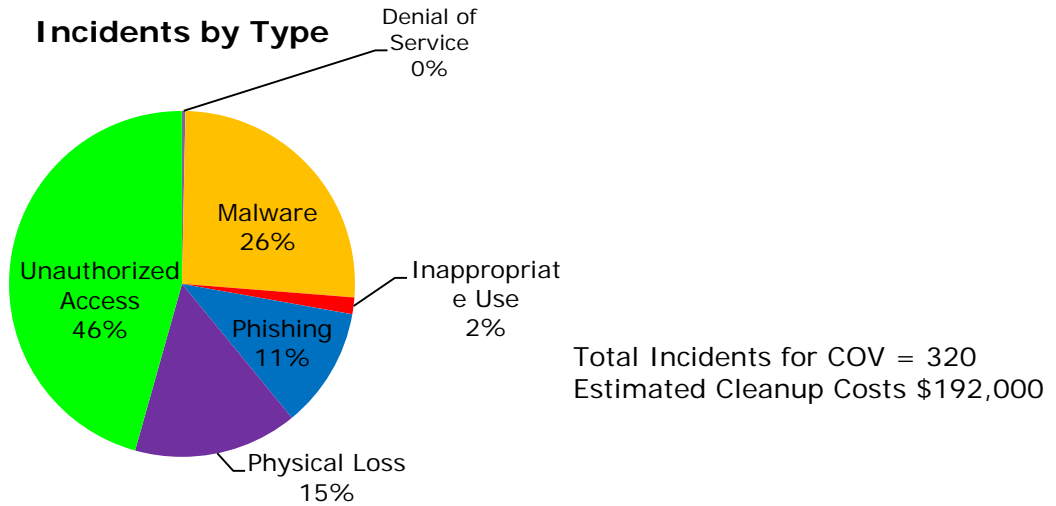
Reported security incidents are grouped into one of the following categories:

- 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, Trojans, ransomware, spyware and key loggers
- 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

During 2016, unauthorized access became the top category for security incidents. Attackers used social engineering attacks and phishing campaigns to harvest user credentials and to gain unauthorized access to COV systems. Malware dropped to second place with physical theft/loss moving into third. The method to address the first place category involves both security awareness training and implementation

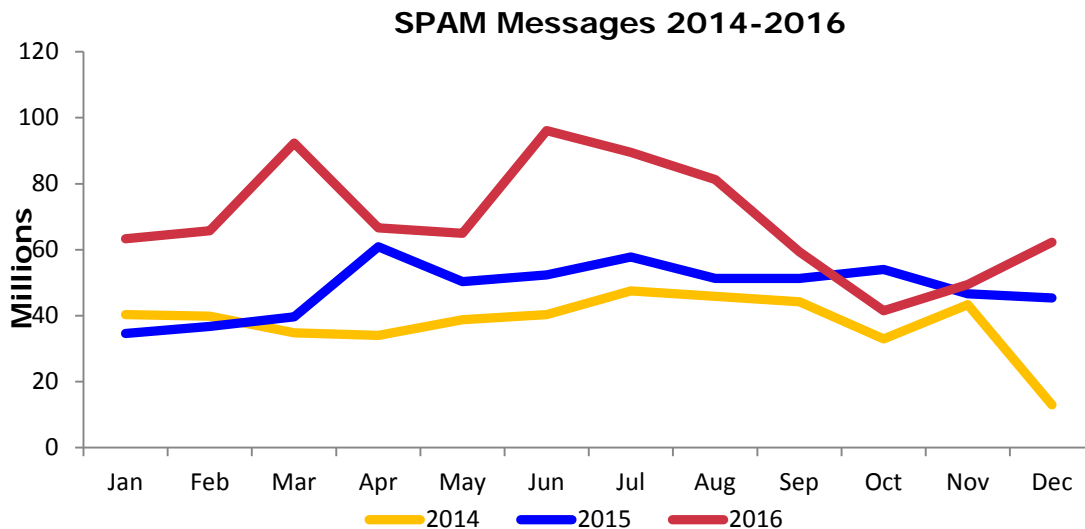


of multifactor authentication. Teaching users to not give away their passwords and to make unique passwords for each user sign-on should help reduce these incidents. Stolen hardware makes up the third place category. Full disk encryption is used to mitigate data loss in hardware thefts; however, as this issue is also due to user behavior, theft prevention should also be included in security awareness training.



SPAM Messages

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 to protect commonwealth information assets. In 2016, the commonwealth filtered more than 832 million spam messages, 90 percent of all email received.

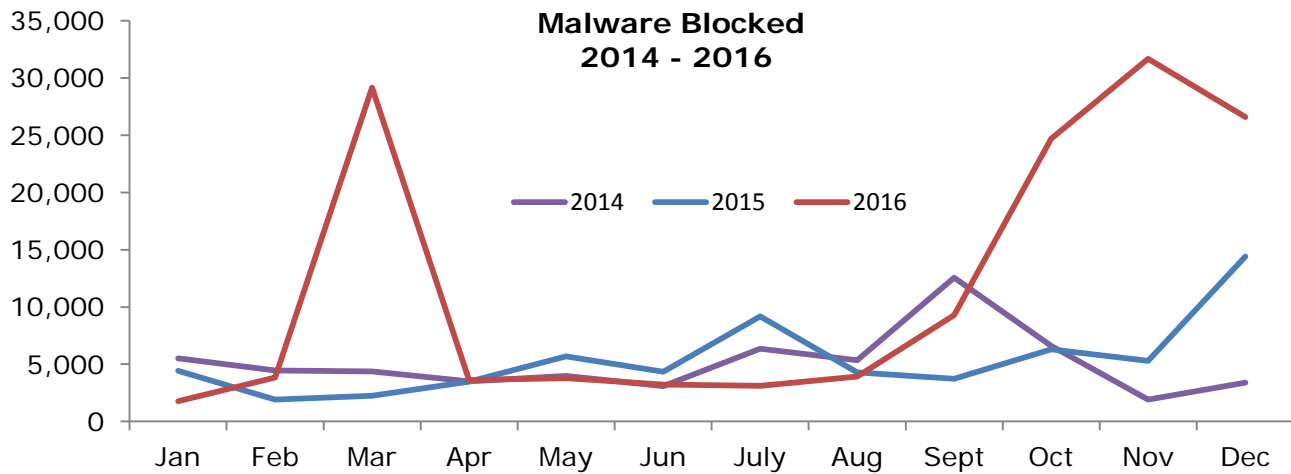




Malware Blocked

While the commonwealth blocked 144,676 pieces of malware from reaching commonwealth assets, this was an increase of 122 percent from 2015., Malware is still ranked as the second largest category of security incidents.

In March 2016, there was an increase in JavaScript Trojans that was detected by McAfee. The fourth quarter of 2016 saw a large increase in malware due to Mal/DropZp-A attack. This Trojan is normally seen as an attachment to spam emails. It uses social engineering to get victims to open the malicious attachment. Once the attachment is open, it downloads malware to the machine. This malware has a direct correlation to the increase in unauthorized access incidents for the fourth quarter of 2016, as both are a result of social engineering attacks.

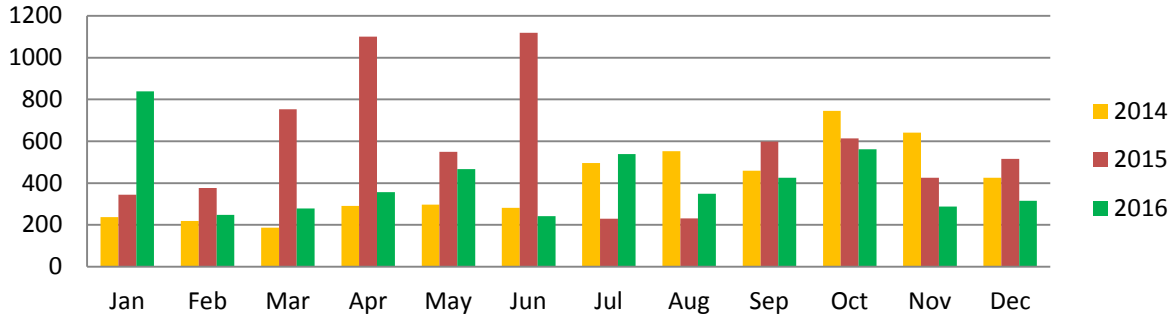


Vulnerability Tracking

As part of tracking threats to the commonwealth, CSRM monitors COV systems for newly discovered vulnerabilities and incorporates them into a weekly advisory. This advisory is distributed to localities, state agencies and higher education. In 2016, the advisory identified 4,907 vulnerabilities that could affect commonwealth systems. ISOs can use this information to ensure that systems are being patched in compliance with security standards.



**Vulnerabilities by Month
2014-2016**

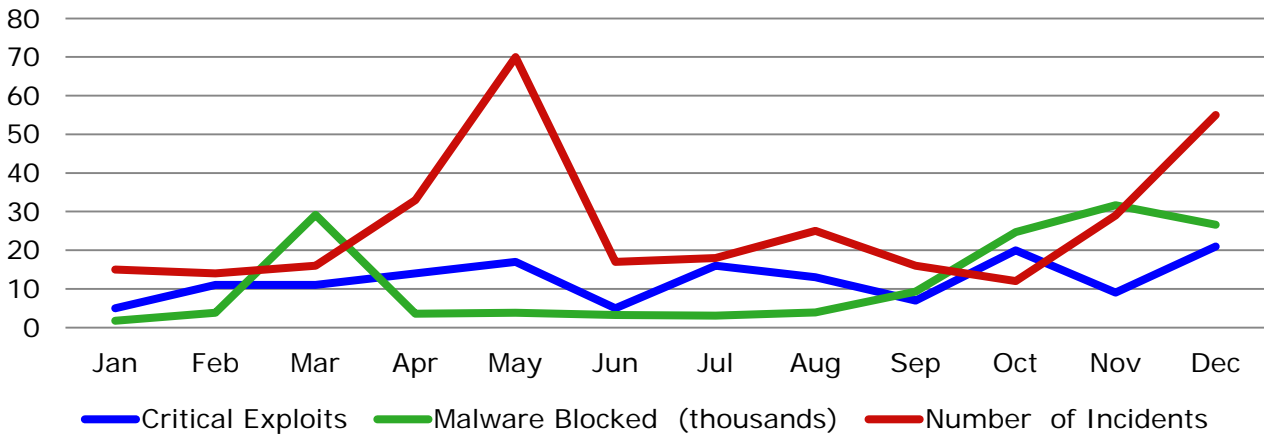


Critical exploits decreased slightly from the previous year

When an attacker finds vulnerabilities before the vendor is aware of it, it is known as a zero-day vulnerability. Attackers develop exploit code using these zero-day vulnerabilities to install malware on a device before the vendor can provide an update or before the update has been installed by the user. As exploit code is available in the wild, these zero-day vulnerabilities pose an increased risk to the environment as seen by the number of malware infections to COV devices.

During 2016, the total number of critical exploits, the opportunities for attackers to exploit the vulnerabilities before they have been identified and fixed by the vendor, decreased slightly from 149 to 132, an 11 percent decrease. However, as summarized on the chart below, critical exploits are correlated to the amount of malware that is blocked and the number of incidents that occur. Attackers use these critical exploits to deliver malware. As malware remains the second largest category for incidents, it is important that critical exploits are patched as soon as possible after appropriate testing to block malware and prevent an increase in incidents.

2016 Critical Exploits, Malware, and Incidents

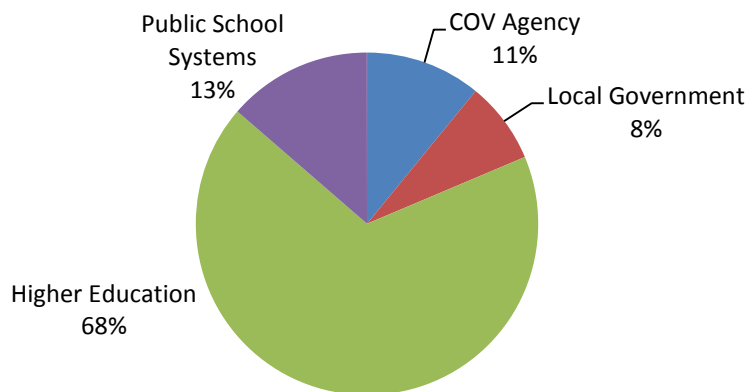




Cyber Intelligence from Commonwealth Partners

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 2016, the commonwealth completed 329 investigations for the alerts that were received. This was a 20 percent decrease from 2015. The following chart shows the percentage of investigations by type of entity.

2016 Percentage of Investigations



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, higher education now leads other public entities in all categories of investigations. As these investigations are comprised solely of the MS-ISAC reported issues, the potential exists for additional security incidents to have been found resulting in a much greater loss. Due to higher education now leading all four investigation categories, we continue to recommend additional guidance for these institutions. It is important to ensure that appropriate governance is established and effective information security programs are implemented in higher education.



Security Investigations by Category

	Higher Education	Local Government	Public School Systems	COV Agencies
Accounts Compromised	85%	4%	7%	4%
Malware Infections	97%	1%	0%	2%
Cyberattacks	53%	21%	5%	21%
Software Vulnerabilities	44%	30%	13%	13%
*Potential Loss Associated with Records Exposed	\$748,176	\$58,960	\$111,408	\$29,920

*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 2016 Cost of a Data Breach Study: Global Analysis report and the number of security investigations.

CSRM Security Services Center

CSRM established additional security services in 2016: IT security audit, ISO services, and vulnerability scanning. In response to agencies that were not able to implement an adequate information security program the governor tasked VITA with establishing an IT security service center and allocated funding to agencies to support these efforts. These services were designed to address the parts of the information security program that the agencies were not able to support.

IT Security Audit Services

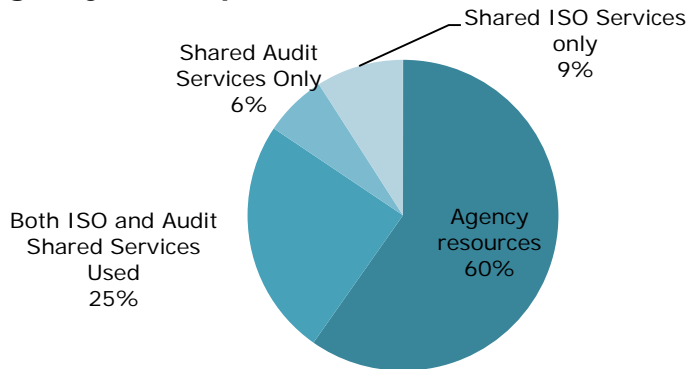
This security offering assists agencies in identifying concerns in their IT security environments. There were 25 agencies that subscribed to this service. Subscribers to the IT security audit service will receive or have received IT security audits of systems that have been identified as sensitive, as well as assistance with compliance with VITA IT security audit program requirements.

ISO Services

There were 26 agencies that elected to participate in the program. Services provided included assistance in developing risk assessment plans, business impact analysis (BIA), and system security plans in an effort help bolster the agencies risk management programs.



Agency Participation in Shared Audit, ISO Services

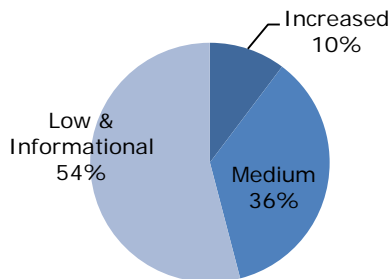


Vulnerability Scanning Services

VITA has also established a program to provide vulnerability scans to commonwealth systems. These vulnerability scans are designed to determine if there are weaknesses in a system that would allow malicious outsiders to attack commonwealth systems and information. CSRM started to perform these scans for all public-facing websites and systems operated by state agencies. To support this effort, VITA worked with agencies to ensure website inventories were complete and accurate. CSRM scheduled the scans to accommodate agency operations and conducted scans each quarter. As a result of this collaboration, CSRM completed the first set of more than 1,300 scans in the last quarter of 2016, with overall compliance rate of 97.50 percent.

The results of the vulnerability scans were alerts that notified agencies of potential security weaknesses that were found in the websites. The alerts were risk rated to convey the potential impact of that vulnerability. Alerts with increased risk had the most risk, while the low and informational risk alerts were deemed to be the least risky.

Vulnerability Scan Alert Summary



More than half of the alerts were related to low risk vulnerabilities

The commonwealth has already begun to reap the benefits of the scanning service. Agencies deactivated websites that were no longer used, resulting in a reduction in the commonwealth’s threat surface. Agencies also began to remediate the vulnerabilities that were identified during the scans. This has further reduced the ability for potential



attackers to exploit these vulnerabilities and access sensitive information. CSRM has also encouraged agencies to prioritize their remediation efforts and address the vulnerabilities by risk, addressing the highest risk vulnerabilities first, dedicating appropriate resources commensurate with the risk posed to commonwealth information.

Commonwealth Information Security Governance Program

The commonwealth's information security governance program is responsible for monitoring performance and compliance against IT security policies and standards, setting security strategy for the commonwealth, supporting agencies in their efforts to foster secure IT security environments, and promoting information security training and awareness.

Statute Requires Compliance Monitoring

As directed by §2.2-2009 (B.1) of the Code of Virginia, the CIO is required to report the "results of security audits, the extent to which security policy, standards, and guidelines have been adopted by executive branch and independent agencies, and a list of those executive branch agencies and independent agencies that have not implemented acceptable security and risk management regulations, policies, standards, and guidelines to control unauthorized uses, intrusions, or other security threats." CSRM accomplished this task by monitoring agencies' overall compliance with IT audit program and information security risk program standards and policies. In addition CSRM started transitioning toward a maturity model which provides additional insight into agency programs. This insight will help show where the commonwealth can direct efforts to further the security program.

Key Commonwealth Security Audit Compliance Metrics and Analysis

Metrics are summarized below to illustrate the results of IT audit program compliance, security trends, and emerging issues as reported by state agencies.

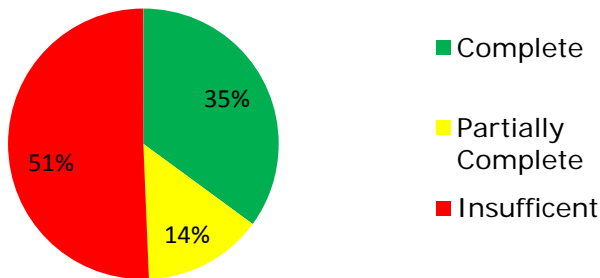
Commonwealth information security audit program compliance increased slightly in 2016. The commonwealth's IT security audit standards dictate that agency heads are accountable for their cybersecurity programs. Agencies are required to develop and maintain an IT security audit program to assess their sensitive systems. Agencies are required to 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 carry out corrective action plans for findings noted during the audits.

There was a slight increase in the overall audit program compliance from the prior year, with 35 percent of agencies having implemented a comprehensive audit program in 2016, compared to 34 percent of agencies with a sufficient audit program last year. When audits are not completed as required, it impacts the



commonwealth’s ability to determine if effective security controls have been designed or implemented by the agencies. With the recent establishment of VITA IT security audit services there should be a steady increase due to the assistance to the agencies in completing the audits and identifying information security risks that need to be mitigated. The complete results will be more apparent at the end of the three-year audit cycle; however, indicators of progress should begin to show as soon as 2017.

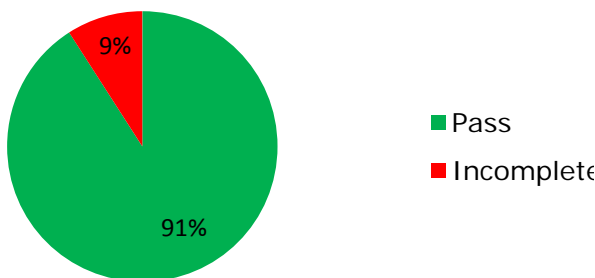
Audit Program Compliance



Overall audit program compliance increased by 1 percent

Agencies that conduct audits continue to submit their current IT security audit plans. Each agency is required by Information Security Audit Standard SEC502-02.3 to develop an IT security audit plan based on the agency’s data classification and BIA. The agencies are required to submit their IT security audit plans to VITA that include plans to audit their sensitive systems at least once every three years. The IT security audit plans demonstrate that the agencies intend to allocate the appropriate resources to complete their audits of sensitive information within the required timeframes. The agencies that have completed audit plans have increased by 8 percent from last year. This improvement was influenced by five agencies that participated in the centralized audit and/or centralized ISO services that had incomplete audit plans in the prior year and have completed IT security audit plans in the current year.

Audit Plan Status

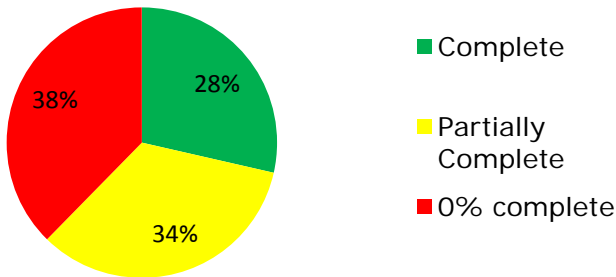


IT security audit plans submitted increased by 8 percent



Most agencies did not complete required audits within the timeframes mandated by commonwealth standards. As previously 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 agencies that have established an audit plan, 28 percent have fulfilled the obligation to have every sensitive system audited at least once every three years, and 34 percent have partially fulfilled their audit obligation and audited some of their applications. As agencies begin to complete their IT security audits with the additional IT security service funding that they have been given, CSRSM anticipates this metric will begin to improve.

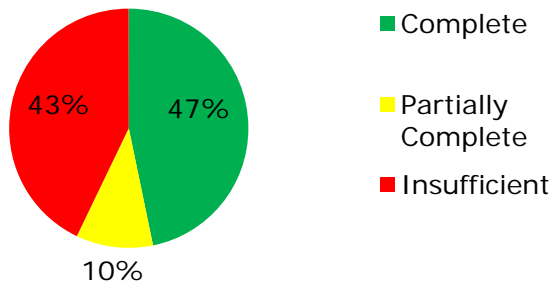
Three Year Audit Obligation



Three year audit obligation completions decreased by 10 percent

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 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.

Current Year Percentage of Audit Reports Received



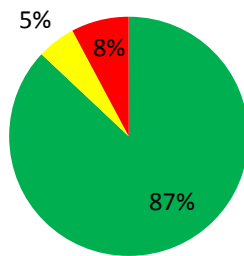
Current year percentage of audit reports decreased by 10 percent



Agencies submitted 2016 quarterly updates for corrective action plans in progress. Agencies are required by SEC502-02.3 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.

The summary includes 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 an overly positive view of compliance. Similar to the other IT security audit metrics, the percentage of quarterly updates received also declined from the prior year. CSRM will further encourage agencies to submit their quarterly updates to ensure that any open control weaknesses in the commonwealth are known and appropriate comprehensive solutions can be developed.

Current Year Percentage of of Quarterly Updates Received



- Complete
- Partially Complete
- Insufficient



Quarterly updates received increased by 1 percent

Analysis of IT security audits findings revealed over half of open findings were related to Center for Internet Security (CIS) critical controls. CSRM found that 56 percent of open findings were related to CIS critical controls (formerly known as SANS top 20 critical controls). These controls are established, well-recognized information security controls that when properly implemented help organizations better secure their information and protect against cyberattacks. A main benefit of using the CIS critical controls as a basis of the IT security program is that these controls focus on a smaller number of actions/steps that will have high pay-off in terms of results. CSRM encourages agencies to remediate all of their findings in a timely manner, placing priority on the remediation of any deficiencies related to CIS critical controls to use IT resources efficiently and effectively.

Commonwealth Information Security Officers Advisory Group

The Information Security Officers Advisory Group (ISOAG) is a dynamic group of information security professionals, open to all state and local government personnel. The group’s goal is to exchange IT security knowledge to improve the security posture of the commonwealth. In 2016, CSRM provided knowledgeable speakers from government and private sector organizations to share their information security expertise with the group at



no cost to attendees. In addition, the members are able to earn continuing professional education credits (CPE), a requirement necessary for security professionals to maintain their security certifications and memberships in global security organizations, share best practices, provide feedback on proposed policy changes, and are notified of local training opportunities. There was an average of 144 attendees per meeting in 2016, which is a 3 percent increase in attendance from the prior year. Members can attend the meetings in person or via webinar. Meeting presentation materials are also posted to the VITA website as an additional resource to the group.

Cybersecurity Strategy Development and Monitoring

CSRM continues to develop an overall commonwealth cybersecurity strategy to address the security needs for the commonwealth. The primary objectives for the cybersecurity strategy are:

- Establish a risk-based approach to cyber investment
- Evolve the security operations program
- 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

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. In addition, templates are also available to help agencies develop their own policies.

In 2016, 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, and 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 developed and published the “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 standard directs agencies to ensure that the appropriate information security and risk management activities are 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.

Commonwealth Information Security (IS) Council

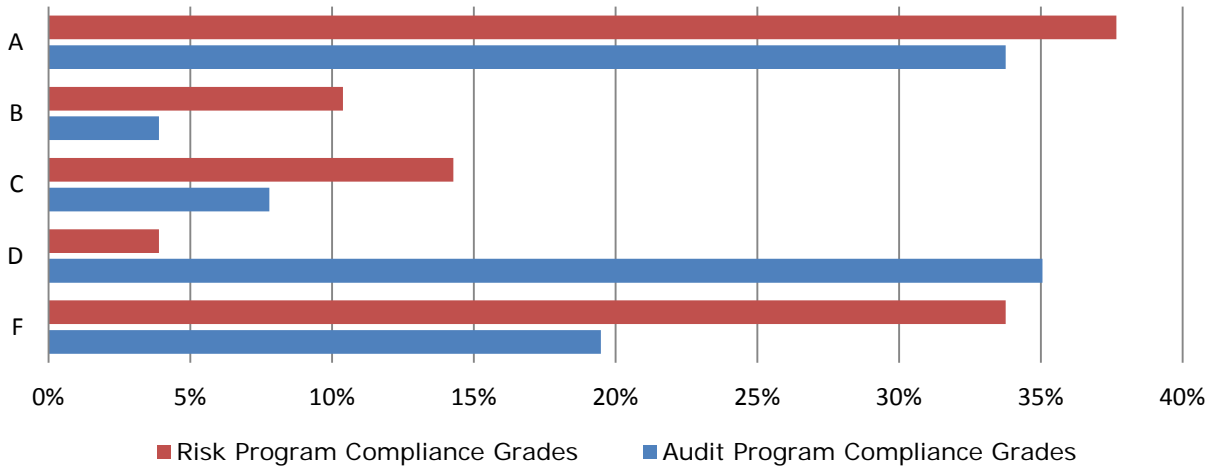
The Commonwealth IS Council is comprised of members from various branches of government. The IS Council’s purpose is to provide input for the direction of the commonwealth-wide information security program and to raise information security awareness within the commonwealth. The IS Council meets twice a month. This year they worked on various initiatives, with the 2016 COV Information Security Conference being a key accomplishment. This sold-out conference supported attendees with responsibilities for managing, auditing or assessing information security in their organizations by providing them information to help them accomplish their tasks more efficiently and effectively. The ISO Council also supports the ISO knowledge sharing website, a site dedicated to promoting communication and information sharing between ISOs.

Compliance Report Card

As part of maturing the information security program CSRM will begin providing more details regarding each agency’s information security program maturity. In order for CSRM to identify the maturity level of the program, the program has to meet the minimum compliance requirements established. CSRM has established a score card for the information provided as part of the compliance documentation. The compliance score card includes the results of each agency’s compliance with IT security audit and risk management requirements. This new metric is intended to provide a better understanding of and additional detail to further describe the state of the IT security audit and risk programs in the commonwealth. Overall commonwealth compliance results indicate that while some agencies have established programs and practices that meet commonwealth security requirements, most agencies have not yet established effective IT security and/or risk management program, earning a grade of C or below. CSRM anticipates that as these agencies begin to implement additional security tools and strategies with the IT security funds afforded them in the recent biennial budget, improved security practices and agency compliance will follow.



Percent of Agencies Earning Each Compliance Grade



Commonwealth IT Risk Management Program

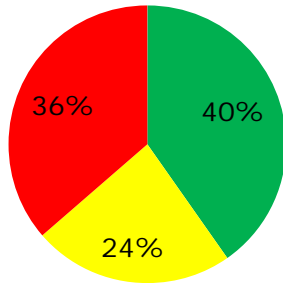
The commonwealth IT Risk Management program provides oversight of the agencies’ risk management programs, including submission of their BIA, risk assessments, and intrusion detection reporting. In addition, CSRM collected sets of data from agencies’ existing BIAs, risk assessments and data on vulnerabilities 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.

IT Risk Management Program Monitoring

Overall risk management program compliance continues to be low. While there was an increase of 5 percent over the prior year, overall risk program compliance continues to lag, with only 40 percent of agencies having implemented a comprehensive risk management program. Agencies should work to conduct their risk assessments on a timely basis and complete their BIA accurately to improve their overall risk programs. CSRM recommends that agencies dedicate the necessary resources to develop their risk programs to sufficiently protect commonwealth systems and information.



Risk Program Compliance



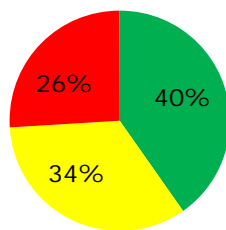
- Complete
- Partially Complete
- Insufficient



Overall risk program compliance increased by 5 percent

Three year risk assessment obligation compliance has improved; however, most agencies still have not met this obligation. Agencies are required by SEC520-00.1 to review their risk assessment plans for the IT systems for which they are 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.

Three Year Risk Assessment Obligation



- Complete
- Partially Complete
- Insufficient



Three year risk assessment obligation increased by 5 percent

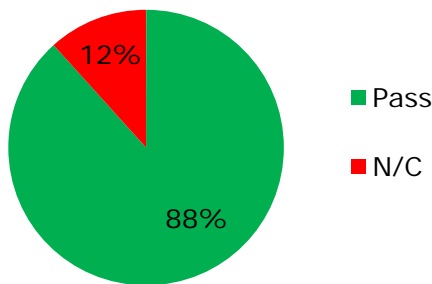
There was no change in the number of agencies with a certified ISO.

Commonwealth ISO certification demonstrates information security training, as well as knowledge of commonwealth information security practices. This expertise and assurance is necessary to lead agencies' information security programs to protect the confidentiality, integrity and availability of the commonwealth's information assets. Agencies that did not have certified ISOs on staff had an average audit compliance of less than 50 percent and an average risk management compliance rate of less than 30 percent. CSRM recommends that these agencies dedicate the necessary resources to obtain certified ISO staff to support their agencies IT security efforts. The following agencies do not have certified ISOs at the conclusion of 2016:



- Tobacco Region Revitalization Commission
- Virginia Resources Authority
- Science Museum of Virginia
- Virginia Commission for the Arts
- Virginia School for the Deaf and Blind
- Office of the Attorney General
- Virginia Foundation for Healthy Youth
- Indigent Defense Commission
- Commonwealth's Attorney's Service Council

ISO Certification Status

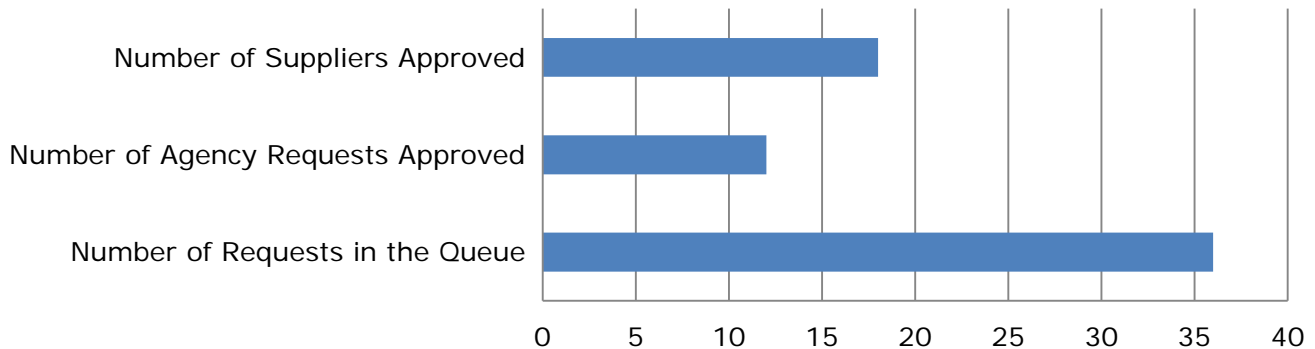


No change in the percentage of certified ISOs

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 implemented third party hosting services to provide security and operational oversight of software as a service solutions. Since the inception of the program, CSRM supported efforts to review suppliers and review and agency requests.



Software as a Service Support



Cybersecurity Framework Assessment

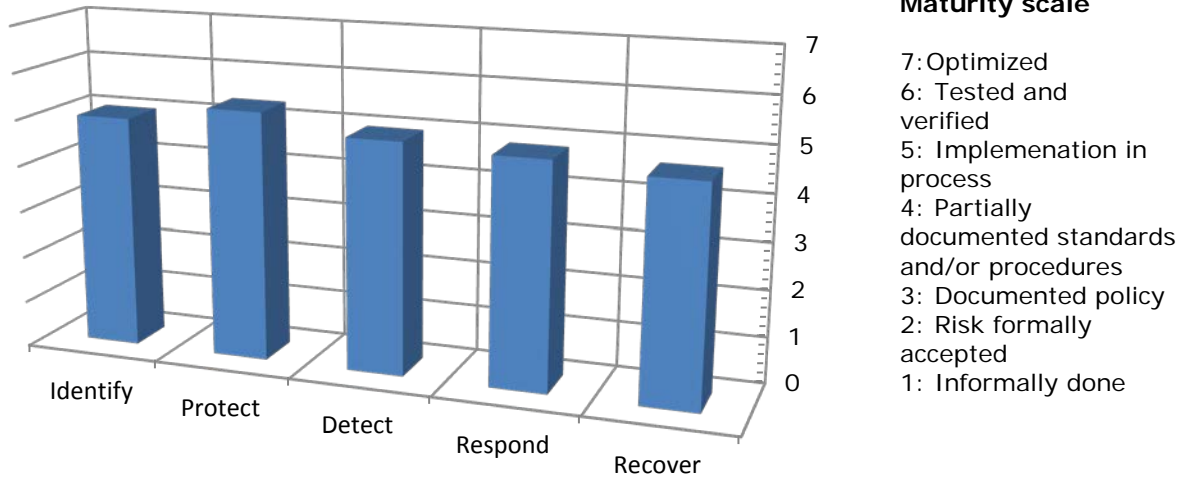
CSRM encouraged agency participation in the Nationwide Cybersecurity Review (NCSR), a survey designed to evaluate organizations' cybersecurity posture. The NCSR is designed based on the NIST Cybersecurity framework to provide insight into the maturity of each agency's information security implementation. The use of the framework helps describe the effectiveness of an agency information security program. It goes one step beyond whether an agency has completed the basic portions of the information security program reflected in the compliance section by providing a scale of what degree the program is implemented at the agency. The NCSR results are an initial attempt at showing some of the progress made by agencies. The assessment is designed to assist agencies in determining their cybersecurity risks and contribute to the nation's cyber risk assessment process. Agencies can use the assessment to identify their target maturity. In the future CSRM will refine the use of assessments against the framework and identify targeted levels of maturity for agencies to reach. The framework is only useful if agencies maintain a basic information security program.

The framework focused on the following core functions: identify, protect, detect, respond and recover. When considered together, an evaluation of these functions provided a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

There were 53 agencies (69 percent) that completed the assessment as required. Survey results, the commonwealth average by core function, are summarized in the chart below. More detailed results by agency are included in Appendix II- Cybersecurity Framework – Dashboard.



NCSR Survey Results



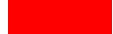



The survey results indicate that on average agencies indicated that they have generally taken some formal steps to have their objectives documented in policy, standards and/or procedures, as well as started the steps to implement them to achieve their objectives. Furthermore, agencies are nearing the implementation phase in their program maturity.




Appendix I - Agency Information Security Data Points - Dashboard





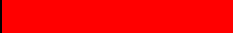

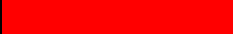















Agency Information Security Data Points Dashboard - Legend

2016 Overall Audit Program

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

2016 Overall Risk Profile

-  - All documentation received as requested information about the agency's vulnerability scans, business impact analysis (BIA), risk assessment(s) (RA) and intrusion detection system (IDS) reports
-  - Partially submitted requirements
-  - Missing any required documentation as requested information about the agency's BIA, RA(s), ISO, or IDS reports

Agency Secretariat	Agency Name	Agency Acronym	Audit Program Compliance	Audit Grade	Risk Program Compliance	Risk Grade
Administration	Compensation Board	CB		A		F
Administration	Department of General Services	DGS		D		C
Administration	Department of Human Resource Management	DHRM		D		A
Administration	Department of Elections	ELECT		D		A
Agriculture & Forestry	Department of Forestry	DOF		A		C
Agriculture & Forestry	Virginia Department of Agriculture and Consumer Services	VDACS		A		A
Agriculture & Forestry	Virginia Racing Commission	VRC		A		A
Commerce and Trade	Board of Accountancy	BOA		A		A
Commerce and Trade	Department of Housing and Community Development	DHCD		D		C
Commerce and Trade	Department of Mines, Minerals and Energy	DMME		F		F
Commerce and Trade	Department of Labor and	DOLI		D		B

COV: Agency Data Points

Agency Secretariat	Agency Name	Agency Acronym	Audit Program Compliance	Audit Grade	Risk Program Compliance	Risk Grade
	Industry					
Commerce and Trade	Department of Professional and Occupational Regulation	DPOR		A		A
Commerce and Trade	Department of Small Business and Supplier Diversity	SBSD		D		A
Commerce and Trade	Tobacco Region Revitalization Commission	TRRC		D		F
Commerce and Trade	Virginia Employment Commission	VEC		D		F
Commerce and Trade	Virginia Economic Development Partnership	VEDP		D		F
Commerce and Trade	Virginia Resources Authority	VRA		F		F
Education	Department of Education	DOE		A		F
Education	Frontier Culture Museum of Virginia	FCMV		D		A
Education	Gunston Hall	GH		D		A
Education	Jamestown-Yorktown Foundation	JYF		D		B
Education	Library of Virginia	LVA		D		F
Education	Norfolk State University	NSU		F		F
Education	Richard Bland College	RBC		A		F
Education	State Council of Higher Education for Virginia	SCHEV		F		F
Education	Science Museum of Virginia	SMV		C		F
Education	Southern Virginia Higher Education Center	SVHEC		A		A
Education	Virginia Commission for the Arts	VCA		F		F
Education	Virginia Museum of Fine	VMFA		F		F

COV: Agency Data Points

Agency Secretariat	Agency Name	Agency Acronym	Audit Program Compliance	Audit Grade	Risk Program Compliance	Risk Grade
	Arts					
Education	Virginia School for the Deaf and Blind	VSDB		F		F
Education	Virginia State University	VSU		A		D
Executive	Office of the Governor	GOV		D		A
Executive	Office of Attorney General	OAG		F		F
Executive	Office of State Inspector General	OSIG		A		A
Finance	Department of Accounts	DOA		C		C
Finance	Department of Planning and Budget	DPB		D		A
Finance	Department of Taxation	TAX		A		F
Finance	Department of Treasury	TD		A		A
Health and Human Resources	Office of Children's Services	CSA		D		A
Health and Human Resources	Department for Aging and Rehabilitative Services	DARS		A		C
Health and Human Resources	Department of Behavioral Health and Development Services	DBHDS		D		B
Health and Human Resources	Department for the Deaf and Hard of Hearing	DDHH		D		B
Health and Human Resources	Department of Health Professions	DHP		A		A
Health and Human Resources	Department of Medical Assistance Services	DMAS		B		F
Health and Human Resources	Department of Social Services	DSS		B		C
Health and Human Resources	Virginia Department of Health	VDH		F		F

COV: Agency Data Points

Agency Secretariat	Agency Name	Agency Acronym	Audit Program Compliance	Audit Grade	Risk Program Compliance	Risk Grade
Health and Human Resources	Virginia Foundation for Healthy Youth	VFHY		F		F
Independent	Indigent Defense Commission	IDC		F		F
Independent	State Corporation Commission	SCC		A		D
Independent	State Lottery Department	SLD		C		F
Independent	Virginia College Savings Plan	VCSP		A		A
Independent	Virginia Retirement System	VRS		A		B
Independent	Virginia Workers Compensation Commission	VWC		C		A
Natural Resources	Department of Conservation and Recreation	DCR		A		A
Natural Resources	Department of Environmental Quality	DEQ		F		C
Natural Resources	Department of Game and Inland Fisheries	DGIF		D		D
Natural Resources	Department of Historic Resources	DHR		F		C
Natural Resources	Marine Resources Commission	MRC		D		A
Natural Resources	Virginia Museum of Natural History	VMNH		D		A
Public Safety	Alcoholic Beverage Control	ABC		F		B
Public Safety	Commonwealths Attorneys Services Council	CASC		A		F
Public Safety	Department of Criminal Justice Services	DCJS		A		B
Public Safety	Department of Fire Programs	DFP		D		C

COV: Agency Data Points

Agency Secretariat	Agency Name	Agency Acronym	Audit Program Compliance	Audit Grade	Risk Program Compliance	Risk Grade
Public Safety	Department of Forensic Science	DFS		D		B
Public Safety	Department of Juvenile Justice	DJJ		A		A
Public Safety	Department of Military Affairs	DMA		F		C
Public Safety	Department of Corrections	DOC		A		A
Public Safety	Virginia Department of Emergency Management	VDEM		D		F
Public Safety	Virginia State Police	VSP		C		A
Technology	Center for Innovative Technologies	IEIA		D		A
Technology	Virginia Information Technologies Agency	VITA		A		A
Transportation	Department of Motor Vehicles	DMV		C		A
Transportation	Department of Aviation	DOAV		A		A
Transportation	Department of Rail and Public Transportation	DRPT		D		F
Transportation	Motor Vehicle Dealer Board	MVDB		D		F
Transportation	Virginia Department of Transportation	VDOT		B		C
Veterans and Defense Affairs	Department of Veterans Services	DVS		A		A

Appendix II - Agency Information Security Data Points - Detail

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

2016 Audit Plan Status

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

2016 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 complete IT 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 Three 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 Three Year Risk Assessment Obligation Completed

- X% - The percentage of risk assessment work completed as measured against the agency's sensitive systems over the past three years
- N/A - Not applicable as the agency had no risk assessments due
- N/C - The agency head has not submitted an audit plan

Agency Secretariat	Agency Acronym	Audit (A) and/or ISO (I) Shared Services	Audit Plan Status	Current Year Percentage of Audit Reports Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	ISO Certification Status
Administration	CB		Pass	N/A	N/A	100%	N/C	N/C	N/C	Pass	Pass
Administration	DGS		Pass	0%	N/A	20%	Pass	0%	Pass	Pass	Pass
Administration	DHRM	A, I	Pass	0%	N/A	5%	Pass	100%	Pass	Pass	Pass
Administration	ELECT	I	Pass	0%	0%	100%	Pass	75%	Pass	Pass	Pass
Agriculture & Forestry	DOF	A, I	Pass	100%	100%	79%	Pass	80%	N/C	Pass	Pass
Agriculture & Forestry	VDACS		Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Agriculture & Forestry	VRC	A, I	Pass	0%	N/A	N/A	Pass	N/A	Pass	Pass	Pass
Commerce and Trade	BOA	A, I	Pass	N/A	100%	100%	Pass	100%	Pass	Pass	Pass
Commerce and Trade	DHCD	A	Pass	0%	N/A	0%	Pass	0%	Pass	Pass	Pass
Commerce and Trade	DMME	A, I	Pass	N/A	0%	0%	N/C	N/C	Pass	Pass	Pass
Commerce and Trade	DOLI	A, I	Pass	N/A	N/A	0%	Pass	12%	Pass	Pass	Pass
Commerce and Trade	DPOR		Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Commerce and Trade	SBSD	A, I	Pass	0%	N/A	0%	Pass	100%	Pass	Pass	Pass
Commerce and Trade	TRRC		Pass	N/C	N/A	N/C	Pass	N/A	N/C	Pass	N/C
Commerce and Trade	VEC		Pass	40%	100%	10%	N/C	N/C	Pass	Pass	Pass
Commerce and Trade	VEDP		Pass	0%	N/A	0%	N/C	N/C	N/C	Fail	Pass

Agency Secretariat	Agency Acronym	Audit (A) and/or ISO (I) Shared Services	Audit Plan Status	Current Year Percentage of Audit Reports Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	ISO Certification Status
Commerce and Trade	VRA		N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	N/C
Education	DOE	A, I	Pass	0%	100%	91%	Pass	0%	N/C	Pass	Pass
Education	FCMV	I	Pass	0%	N/A	0%	Pass	100%	Pass	Pass	Pass
Education	GH	I	Pass	0%	N/A	0%	Pass	100%	Pass	Pass	Pass
Education	JYF	A, I	Pass	0%	N/A	17%	Pass	17%	Pass	Pass	Pass
Education	LVA		Pass	0%	N/A	5%	Pass	0%	N/C	Pass	Pass
Education	NSU	A, I	N/C	N/C	N/A	N/C	N/C	N/C	Incomplete	Pass	Pass
Education	RBC		Pass	100%	100%	100%	N/C	N/C	N/C	Pass	Pass
Education	SCHEV	A, I	Pass	N/A	0%	25%	N/C	N/C	N/C	Pass	Pass
Education	SMV		Pass	100%	N/A	17%	N/C	N/C	N/C	Pass	N/C
Education	SVHEC	I	Pass	N/A	N/A	N/A	Pass	N/A	Pass	Pass	Pass
Education	VCA		N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	N/C
Education	VMFA		Pass	N/A	0%	0%	N/C	N/C	N/C	Pass	Pass
Education	VSDB		N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	N/C
Education	VSU	A, I	Pass	100%	100%	82%	Pass	9%	N/C	Pass	Pass
Executive	GOV	I	Pass	0%	N/A	0%	Pass	100%	Pass	Pass	Pass
Executive	OAG		N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	N/C
Executive	OSIG		Pass	100%	N/A	100%	Pass	100%	Pass	Pass	Pass
Finance	DOA	A	Pass	100%	100%	40%	Pass	0%	Pass	Pass	Pass
Finance	DPB	A, I	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Pass
Finance	TAX		Pass	100%	100%	92%	Pass	0%	N/C	Pass	Pass
Finance	TD		Pass	100%	100%	100%	Pass	73%	Pass	Pass	Pass
Health and Human Resources	CSA		Pass	N/A	0%	100%	Pass	100%	Pass	Pass	Pass

Agency Secretariat	Agency Acronym	Audit (A) and/or ISO (I) Shared Services	Audit Plan Status	Current Year Percentage of Audit Reports Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	ISO Certification Status
Health and Human Resources	DARS		Pass	100%	100%	88%	Pass	7%	Incomplete	Pass	Pass
Health and Human Resources	DBHDS		Pass	25%	N/A	0%	Pass	4%	Pass	Pass	Pass
Health and Human Resources	DDHH	A	Pass	N/C	N/A	N/C	Pass	25%	Pass	Pass	Pass
Health and Human Resources	DHP		Pass	100%	N/A	100%	Pass	100%	Pass	Pass	Pass
Health and Human Resources	DMAS		Pass	25%	100%	72%	N/C	N/C	N/C	Pass	Pass
Health and Human Resources	DSS		Pass	100%	75%	67%	Pass	0%	Pass	Pass	Pass
Health and Human Resources	VDH		Pass	88%	100%	36%	Pass	0%	N/C	Pass	Pass
Health and Human Resources	VFHY		N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	N/C
Independent	IDC		N/C	N/C	N/A	N/C	Pass	100%	N/C	Pass	N/C
Independent	SCC		Pass	89%	100%	86%	Pass	0%	Incomplete	Pass	Pass
Independent	SLD		Pass	29%	100%	26%	N/C	N/C	N/C	Fail	Pass
Independent	VCSP		Pass	0%	100%	100%	Pass	100%	Pass	Pass	Pass
Independent	VRS		Pass	100%	100%	100%	Pass	100%	Incomplete	Pass	Pass
Independent	VWC	A	Pass	0%	N/A	50%	Pass	100%	Pass	Pass	Pass
Natural Resources	DCR	I	Pass	N/A	100%	100%	Pass	100%	Pass	Pass	Pass

Agency Secretariat	Agency Acronym	Audit (A) and/or ISO (I) Shared Services	Audit Plan Status	Current Year Percentage of Audit Reports Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	ISO Certification Status
Natural Resources	DEQ	A, I	Pass	0%	75%	12%	Pass	0%	Pass	Pass	Pass
Natural Resources	DGIF		Pass	100%	0%	35%	Pass	7%	N/C	Pass	Pass
Natural Resources	DHR	A, I	Pass	0%	0%	0%	Pass	0%	Pass	Pass	Pass
Natural Resources	MRC	A	Pass	100%	N/A	12%	Pass	100%	Pass	Pass	Pass
Natural Resources	VMNH	A, I	Pass	N/A	N/A	0%	Pass	100%	Pass	Pass	Pass
Public Safety	ABC		Pass	67%	18%	58%	Pass	75%	Incomplete	Pass	Pass
Public Safety	CASC		Pass	N/A	N/A	N/A	N/C	N/C	N/C	Pass	N/C
Public Safety	DCJS	A, I	Pass	N/A	N/A	N/A	Pass	N/A	Incomplete	Pass	Pass
Public Safety	DFP		Pass	0%	N/A	0%	Pass	0%	Pass	Pass	Pass
Public Safety	DFS	A, I	Pass	0%	N/A	0%	Pass	100%	Incomplete	Pass	Pass
Public Safety	DJJ	I	Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Public Safety	DMA		N/C	N/C	N/A	N/C	Pass	N/A	N/C	Pass	Pass
Public Safety	DOC		Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Public Safety	VDEM		Pass	0%	N/A	0%	N/C	N/C	N/C	Pass	Pass
Public Safety	VSP		Pass	N/A	79%	45%	Pass	93%	Pass	Pass	Pass
Technology	IEIA		Pass	100%	100%	100%	Pass	100%	Pass	Pass	Pass
Technology	VITA		Pass	0%	100%	88%	Pass	94%	Pass	Pass	Pass
Transportation	DMV		Pass	50%	100%	31%	Pass	100%	Pass	Pass	Pass
Transportation	DOAV		Pass	N/A	100%	100%	Pass	100%	Pass	Pass	Pass
Transportation	DRPT		Pass	N/A	N/A	0%	N/C	N/C	N/C	Pass	Pass
Transportation	MVDB	A, I	Pass	N/A	N/A	0%	N/C	N/C	N/C	Pass	Pass
Transportation	VDOT		Pass	0%	100%	72%	Pass	18%	Incomplete	Pass	Pass
Veterans and Defense Affairs	DVS		Pass	N/A	N/A	100%	Pass	100%	Pass	Pass	Pass

Appendix III – Cybersecurity Framework Results - Detail

Agency Name	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Alcoholic Beverage Control	38%	39%	23%	38%	29%
Board of Accountancy	77%	80%	77%	76%	71%
Center for Innovative Technologies	57%	60%	34%	32%	37%
Commonwealths Attorney's Services Council	0%	0%	0%	0%	0%
Compensation Board	0%	0%	0%	0%	0%
Department for Aging and Rehabilitative Services	64%	85%	86%	85%	79%
Department for the Deaf and Hard of Hearing	64%	85%	86%	85%	79%
Department of Accounts	93%	97%	100%	46%	43%
Department of Aviation	77%	76%	50%	62%	50%
Department of Behavioral Health and Development Services	88%	97%	100%	100%	100%
Department of Conservation and Recreation	77%	80%	77%	76%	71%
Department of Corrections	44%	45%	44%	43%	43%
Department of Criminal Justice Services	77%	80%	77%	76%	71%
Department of Education	0%	0%	0%	0%	0%
Department of Elections	77%	80%	77%	76%	71%
Department of Environmental Quality	77%	80%	77%	76%	71%
Department of Fire Programs	0%	0%	0%	0%	0%
Department of Forensic Science	43%	52%	43%	43%	37%
Department of Forestry	77%	80%	77%	76%	71%
Department of Game and Inland Fisheries	0%	0%	0%	0%	0%
Department of General Services	0%	0%	0%	0%	0%
Department of Health Professions	67%	60%	50%	55%	40%
Department of Historic Resources	71%	54%	68%	65%	83%
Department of Housing and Community Development	43%	0%	0%	0%	0%
Department of Human Resource Management	75%	79%	76%	71%	71%
Department of Juvenile Justice	77%	80%	77%	76%	71%
Department of Labor and Industry	77%	80%	77%	76%	71%
Department of Medical Assistance Services	73%	87%	75%	80%	48%
Department of Military Affairs	0%	0%	0%	0%	0%
Department of Mines, Minerals and Energy	79%	83%	75%	73%	78%
Department of Motor Vehicles	77%	75%	68%	83%	71%
Department of Planning and Budget	70%	71%	73%	66%	81%
Department of Professional and Occupational Regulation	0%	0%	0%	0%	0%
Department of Rail and Public Transportation	51%	52%	48%	54%	43%
Department of Small Business and Supplier Diversity	77%	80%	77%	76%	71%
Department of Social Services	53%	65%	52%	41%	40%
Department of Taxation	95%	99%	100%	100%	100%
Department of Treasury	71%	88%	92%	71%	43%
Department of Veterans Services	43%	59%	63%	62%	43%
Frontier Culture Museum of Virginia	77%	80%	77%	76%	71%
Gunston Hall	71%	66%	70%	66%	59%
Indigent Defense Commission	78%	87%	74%	60%	45%
Jamestown-Yorktown Foundation	77%	76%	77%	76%	71%
Library of Virginia	52%	73%	62%	60%	62%
Marine Resources Commission	83%	79%	73%	83%	79%
Motor Vehicle Dealer Board	77%	80%	77%	76%	71%
Norfolk State University	77%	80%	77%	76%	71%
Office of Attorney General	0%	0%	0%	0%	0%
Office of Children's Services	83%	89%	83%	84%	86%
Office of State Inspector General	100%	85%	100%	100%	100%
Office of the Governor	68%	74%	75%	75%	71%
Richard Bland College	0%	0%	0%	0%	0%
Science Museum of Virginia	0%	0%	0%	0%	0%
Southern Virginia Higher Education Center	71%	67%	71%	63%	43%
State Corporation Commission	0%	0%	0%	0%	0%
State Council of Higher Education for Virginia	77%	80%	77%	76%	71%
State Lottery Department	76%	79%	74%	0%	100%
Tobacco Region Revitalization Commission	0%	0%	0%	0%	0%
Virginia College Savings Plan	91%	99%	100%	97%	81%
Virginia Commission for the Arts	0%	0%	0%	0%	0%
Virginia Department of Agriculture and Consumer Services	50%	80%	25%	78%	71%
Virginia Department of Emergency Management	25%	0%	0%	0%	0%
Virginia Department of Health	72%	78%	71%	73%	64%
Virginia Department of Transportation	54%	58%	32%	36%	48%
Virginia Economic Development Partnership	0%	0%	0%	0%	0%
Virginia Employment Commission	43%	58%	24%	48%	57%
Virginia Foundation for Healthy Youth	0%	0%	0%	0%	0%
Virginia Information Technologies Agency	91%	96%	99%	92%	98%
Virginia Museum of Fine Arts	0%	0%	0%	0%	0%
Virginia Museum of Natural History	77%	80%	77%	76%	71%
Virginia Racing Commission	77%	80%	77%	76%	71%
Virginia Resources Authority	0%	0%	0%	0%	0%
Virginia Retirement System	0%	0%	0%	0%	0%
Virginia School for the Deaf and Blind	0%	0%	0%	0%	0%
Virginia State Police	76%	96%	86%	71%	86%
Virginia State University	77%	80%	77%	76%	71%
Virginia Workers Compensation Commission	0%	0%	0%	0%	0%

NOTE: 0% indicates that the agency did not complete that portion of the questionnaire.