VIRGINIA
IT AGENCY

2023
Commonwealth of Virginia
Information Security Report

This report has been submitted in compliance with the Code of Virginia (§2.2-2009).

Comments are welcome. Please send electronic comments to: cio@vita.virginia.gov.

Please submit written correspondence to: Chief Information Officer, Virginia Information Technologies Agency, 7325 Beaufont Springs Drive, Richmond, VA 23225

Background

This 2023 Commonwealth of Virginia (COV) Information Security Report is the 14th 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 shall annually report to the Governor, the Secretary, and General Assembly on 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."*

In addition, this report includes the requirements directed by §2.2-2009(C) of the Code of Virginia, which says: *"The CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures. Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairman of the House Committee on Appropriations and the Senate Committee on Finance. Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities."*

This report combines the requirements of §2.2-2009(B)(1) and §2.2-2009(C) into a single report.

The CIO has established the Commonwealth Security and Risk Management (CSRM) group within the Virginia Information Technologies Agency (VITA) to fulfill statutory information security duties under §2.2-2009. CSRM is led by the Commonwealth's Chief Information Security Officer (CISO).

The scope of this report is limited to the executive branch agencies, six independent agencies, and three Level I institutions of higher education. This report does not address the judicial branch, the legislative branch, nor Level II and Level III higher education institutions, which are either statutorily exempt from compliance with Commonwealth policies and standards or outside the scope of VITA's compliance review.

This report is prepared by CSRM on behalf of the CIO using a series of compliance metrics established by CSRM to assess the strength of the agency information technology (IT) security programs that protect Commonwealth data and systems.

Executive Summary

The Commonwealth's Information Security Program plays a vital role in safeguarding state IT systems by aligning cybersecurity strategies with national standards and fostering collaboration across agencies. The Commonwealth Security and Risk Management (CSRM) division, under the direction of the Chief Information Security Officer and the Chief Information Officer (CIO), oversees this comprehensive program, which is designed to monitor compliance, implement security policies, and enhance training initiatives.

In 2023, the Commonwealth participated in the National Cyber Security Review (NCSR), a self-assessment aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Sponsored by the Multi-State Information Sharing & Analysis Center (MS-ISAC), the NCSR enables agencies to evaluate their cybersecurity posture across five core functions: identify, protect, detect, respond, and recover. Commonwealth agencies performed above the national average, reporting a slight decrease in the overall average score from 5.49 in 2022 to 5.47 in 2023 (on a 7-point scale). The Commonwealth's scores continue to trend higher in the identify and protect functions, while detect, respond, and recover functions remain areas for improvement. Despite these challenges, the Commonwealth ranks higher than peer states, with agencies in sectors like IT and financial services performing particularly well.

The Commonwealth also saw significant progress in other areas in 2023. CSRM expanded its security awareness training platform, integrating simulated phishing campaigns and threat detection exercises to strengthen user knowledge across all agencies. Additionally, VITA's third-party vendors are offering Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) solutions. This ensures security compliance and risk mitigation, particularly in response to the increased demand for cloud services.

Risk management remains a central focus, with the IT Risk Management Committee driving the prioritization of mitigation efforts for significant risks. In 2023, IT risk compliance improved by 27% while audit compliance grades rose by 8%. Although progress has been made, audit findings remain open for an average of 948 days and risk findings for 1,313 days. CSRM recommends agencies continue to monitor their audit and risk management activities closely and implement mitigating controls to address security gaps.

The Commonwealth's shared services model continues to provide key resources for agencies, offering centralized IT security auditing, ISO support, and web application vulnerability scanning. In 2023, over 6,000 public-facing websites were scanned quarterly to identify potential weaknesses and prevent exploitation.

Through the Commonwealth Security Information Council (CISC), the Information Security Officers Advisory Group (ISOAG), and monthly IT Risk Management Committee meetings, CSRM facilitates collaboration and knowledge-sharing across agencies. These forums also allow security professionals to earn continuing professional education credits, further enhancing the Commonwealth's overall cybersecurity maturity.

In conclusion, the Commonwealth's Information Security Program achieved significant progress in 2023. Despite challenges in detect and respond functions, improvements in training, risk management, and third-party oversight have strengthened the Commonwealth's cybersecurity posture. The ongoing participation in the NCSR and other assessment tools will continue to provide valuable insights for agencies to benchmark progress and prioritize areas for improvement in the years ahead.

Commonwealth Threat Management

VITA introduced new monitoring tools in 2023 to improve the COV cybersecurity threat management program.

First, as part of the website modernization program, the web scanning platform was migrated to a cloud solution, allowing agencies to perform evaluations monthly instead of quarterly. While this may decrease the number of vulnerabilities unfound in the environment, it only reduces vulnerability exposure if the application is fixed promptly, ultimately resulting in a significant decrease in the time a website is vulnerable.

Second, CSRM has implemented a log aggregation and monitoring solution. This solution will allow logs to be ingested in their native formats and analyzed for suspicious activity, and alert agencies when defined thresholds are triggered. In addition to assisting agencies with monitoring responsibilities, the tool will enhance the Commonwealth's security posture by aggregating logs from multiple sources, providing a more holistic view of the enterprise. This tool will roll out in 2024.

The third tool introduced by CSRM provides agencies a single pane of glass to review their operating system, application and website vulnerabilities. As scans are conducted, results are loaded into the new tool, allowing agencies to view their risk posture at any time.

The number of physical theft/lost security incidents doubled from 103 to 208 in 2023, making it the leading category of security incidents. These incidents can be prevented by greater user diligence with COV-issued devices, which will avoid concerns about potential data loss. Although full disk encryption mitigates much of the risk, each loss is evaluated to ensure encryption was active and functioning at the time. This control currently applies to laptops, but with the shift to cloud accessibility, additional controls for managing cell phones will roll out in 2024, allowing for remote resets and software management to prevent data loss. Social engineering incidents rose to 102, placing the category in second, while malware ranked third with 78 incidents.

VITA continues to invest in security awareness training to address evolving security concerns. To keep pace with the new threats, CSRM supplements its annual training with simulated phishing exercises. Quarterly phishing campaigns help sharpen users' recognition and incident response skills.

In 2023, attacks against the Commonwealth continued to rise. 106 million attempts were detected -- averaging 3.36 attacks per second, up from 55 million in 2022. Most of these attacks were blocked by Commonwealth monitoring systems and security tools.

Commonwealth Information Security Governance Program

CSRM performs annual compliance reviews of agency information security programs compared to the Commonwealth's IT security policies, standards, and guidelines. Using a letter grade system, agencies receive grades for IT audit and IT risk management programs.

VITA provides education and outreach programs to support information security professionals. CSRM supports multiple events throughout the year to provide training, share enterprise updates, and host networking opportunities for the Commonwealth's security community. Agency personnel regularly participate in councils and committees to provide immediate feedback on various security matters.

Third-party risk management is a key component of the COV Risk Management program. As demand for third-party services continues to increase, VITA consistently assesses all third-party vendors to ensure they operate within risk tolerance thresholds. CSRM integrates with supply chain management and procurement teams, while the Enterprise Cloud Oversight Service (ECOS) (now known as COV Ramp) team reviews and approves contract terms and oversees third-party vendors offering Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) applications.

CSRM offers three centralized security services to customer agencies. The IT Audit, Information Security Officer (ISO), and Web Application Scanning services provide additional support for agency information security programs. The IT Audit and ISO services are subscription-based services to help agencies satisfy specific security requirements. The Web Application Scanning service is provided at no discrete cost to customer agencies. In 2023, the aforementioned scanning tool gave agencies the enhanced ability to conduct their own scans, allowing them to immediately determine the effectiveness of their remediation efforts.

Commonwealth IT Audit and Risk Management Program

IT Audit and Risk compliance grades improved in 2023. The percentage of above average IT audit and IT risk compliance grades improved from 36% in 2022 to 44% in 2023 and from 62% in 2022 to 74% 2023 respectively. CSRM attributes this improvement to the completion of required risk and audit plans and increased compliance monitoring.

CRSM's Risk Management team also monitors the progress and remediation of IT audit and risk findings. In 2023, the average age for all open IT audit and risk findings was 948 and 1,313 days, respectively, which is an increase from 2022. The average age of open IT audit findings increased by 141 days, and the average age of open risk findings increased by 73 days from 2022 to 2023. Most findings resulted from gaps with access control requirements, system integrity (e.g., lacking current security patches), and inadequate third-party hosting agreements. CSRM notifies agencies of outstanding and overdue findings to further encourage agencies to remediate critical findings quickly.

Nationwide Cyber Security Review

The NCSR is a self-assessment survey aligned with the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF). The survey allows CSRM to review how agencies evaluate their own cybersecurity posture and to compare results with other Commonwealth agencies and those from other states. The most current NCSR survey results indicated Commonwealth agencies have an average score (on a scale of 1 to 7) that is slightly better than the national average and that has improved over the prior year. Overall, the average NCSR score for Commonwealth agencies in 2023 was 5.47, which is slightly above the minimum recommended maturity level of 5. Entities at this maturity level have formally documented policies, standards, and procedures and are in the process of implementation. In 2023, 25 Commonwealth agencies participated in the NCSR assessment. More information on NCSR can be found at Nationwide Cybersecurity Review (NCSR) (cisecurity.org)

Conclusions & Recommendations

Centralized Security Awareness Training Platform

User awareness and training is a key defensive measure to help prevent malware-related incidents.

VITA expanded its Security Awareness and Training service to provide a centralized solution available to all Commonwealth agencies, not just executive branch agencies. In 2023, CSRM onboarded customer agencies to the KnowBe4 security awareness training platform. Centralized training modules provides consistent training to the Commonwealth workforce, in compliance with Code of Virginia §2.2-2009(I).

Theft or Loss of Electronic Devices

Lost or stolen physical devices accounted for the majority of the cybersecurity incidents in 2023. Users should familiarize themselves with COV device policies and promptly report any lost or stolen COV devices using the appropriate procedures.

Cybersecurity Attacks & Investigations

VITA detected over 106 million attempted attacks – approximately 3.36 attacks per second. CSRM supported more than 1,000 security investigations on behalf of the Commonwealth in 2023. CSRM recommends agencies identify and implement security controls to reduce the probability and impact of an exploit until security remediation patches can be deployed. CSRM's defense-in-depth approach ensures that the team can implement compensating controls at multiple levels, thereby mitigating threats even when security remediation activities are delayed due to the absence of a patch or other challenges.

IT Compliance Grades

Overall IT Audit and IT Risk compliance grades improved. CSRM will set interim deadlines for agencies throughout the year to track key deliverables and monitor progress.

Nationwide Agency Self-Evaluation

Commonwealth agencies participating in the 2023 NCSR self-assessment tend to assess their compliance with national standards at or above the minimum target score of 5.

Commonwealth Threat Management Report

The Code of Virginia, § 2.2-5514(C), requires all public bodies to report IT security incidents to the Virginia Fusion Intelligence Center, which shares such reports with the CIO, within 24 hours of discovery, in accordance with security standard SEC530. VITA's Computer Security Incident Response Team (CSIRT) then categorizes each security incident based on the type of activity.

In 2023, the Commonwealth continued to support and strengthen its cybersecurity programs and threat management capabilities. Cyberattacks against the Commonwealth of Virginia surged by 90.91%. with over 105 million attack attempts on the network and more than 62,000 pieces of malware blocked. The risk posture was further impacted by a significant rise in lost or stolen devices, such as laptops.

Virginia Cybersecurity Planning Committee (VCPC) & Cybersecurity Grant

In 2022, the Virginia General Assembly directed the Commonwealth's participation in the State and Local Cybersecurity Grant Program (SLCGP), under the Infrastructure Investment and Jobs Act (IIJA), Pub. L. No. 117-58, § 70612 (2021). By November 2022, the Virginia Cybersecurity Planning Committee had been established and begun to meet. The Committee is led by the Commonwealth CISO and consists of an array of state and local cybersecurity leaders from different sectors, appointed by Governor Youngkin. In 2023, the Committee, and then the relevant federal agencies, the Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA), approved Virginia's Cybersecurity Plan, the first whole-of-state approach to cybersecurity in Virginia. The first project under the SLCGP and the Plan has conducted cybersecurity capability assessments for approximately 170 school divisions, local governments, and other public bodies. The Plan and the assessments project enable the Commonwealth to coordinate, prioritize, and utilize cybersecurity resources more efficiently to improve cybersecurity across the Commonwealth. More information about the SLCGP is available in its October 2023 and September 2024 annual reports and on VITA's website, and more information about VCPC meetings may be found on the Virginia Regulatory Town Hall website.

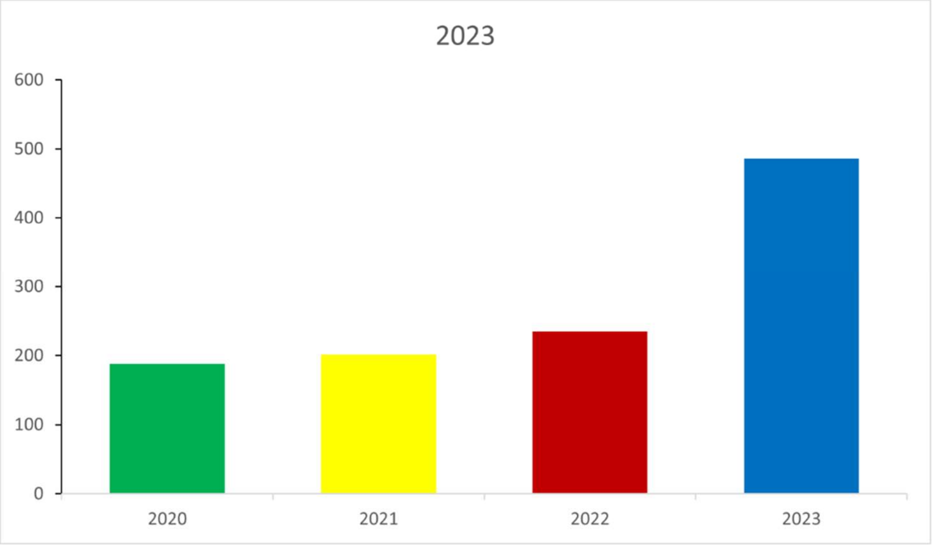
Centralized Incident Reporting: Virginia Fusion Center

To enhance Commonwealth threat intelligence and management, Virginia Code § 2.2-5514 requires all public bodies to report security incidents to the Virginia Fusion Center. Before this requirement, limited incident reporting from localities and higher education institutions reduced visibility into overall Commonwealth risks and hindered the development of effective countermeasures. Since the legislation's enactment, CSRM has begun receiving previously unavailable security incident intelligence from local governments and higher education institutions.

Cybersecurity Incidents

Cybersecurity incidents increased 107% for a total of 486 cybersecurity incidents in 2023. The top three types of incidents were physical loss, social engineering, and malware. Lost or stolen Commonwealth devices rose from 103 to 208, making up 42.8% of incidents. Social engineering incidents jumped from 8 to 102, while malware incidents increased from 52 to 78. Increases in social engineering incidents can be largely attributed to improved reporting as a result of Microsoft's implementation of a phishing alert button (PAB) in its Outlook application. Users that receive a suspicious email can click the PAB to automatically report the incident and remove the email.

Figure 1. Cybersecurity Incidents by Year



As users become more dependent on technology, the risk of physical theft or loss of electronic devices increases. Users frequently utilize laptops, tablets, and smartphones to check email, perform banking transactions, browse the internet, and communicate with colleagues and business partners. With the widespread use of these devices across the Commonwealth, the likelihood of lost or stolen devices is high. If such devices are lost or stolen, the information stored or accessible on them may be compromised. To mitigate the risk of unauthorized disclosure or loss of Commonwealth data, it is crucial to implement and adhere to security controls, such as encryption, and emphasize physical security in awareness training. Physical loss incidents often result from users being unaware of their surroundings and not maintaining custody of their COV-issued devices.

Social engineering incidents increased in 2023. Social engineering incidents rose to second place, accounting for 20.99% of all incidents across the Commonwealth. COV users remain frequent targets, highlighting the need for ongoing security awareness training. The Commonwealth's enterprise-wide security awareness training delivered by CSRM, includes essential components such as:

- Safe browsing habits
- Identifying suspicious emails
- Using email encryption
- Actions to take if something seems suspicious
- How to report incidents

With legislative support, CSRM continues to enhance this program. In 2023, CSRM launched an enterprise-wide platform to deliver consistent training and testing, including simulated phishing campaigns.

More than 62,000 pieces of malware, malicious software, were blocked in 2023. Despite preemptive measures, 16.05% of 2023's cybersecurity incidents were due to malware attacks, which remain pervasive. The rise in malware attacks within the Commonwealth aligns with cyclical patterns of online activity, such as holiday shopping and tax season. Despite the increase in incidents, in 2023 Commonwealth solutions effectively blocked over 99.99% of malware threats.

Figure 2. Cyber Incidents by Category

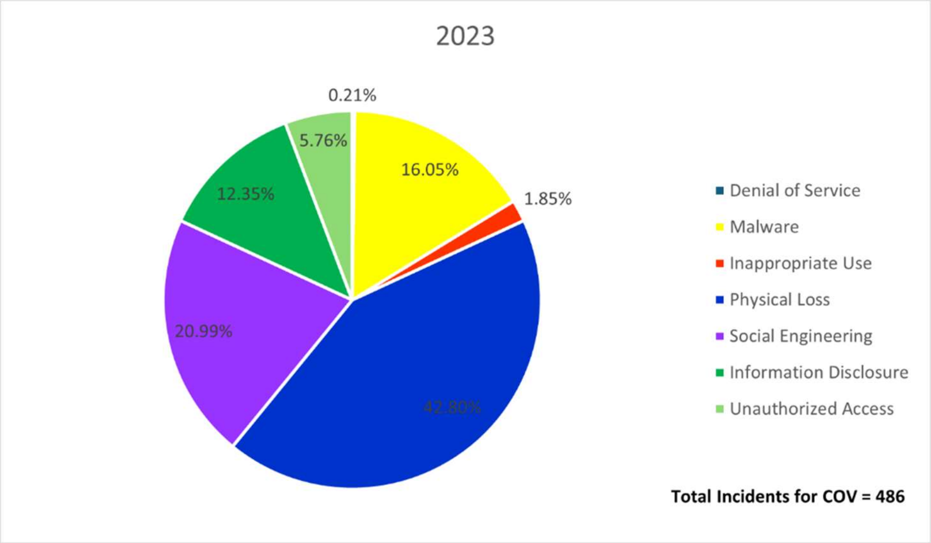
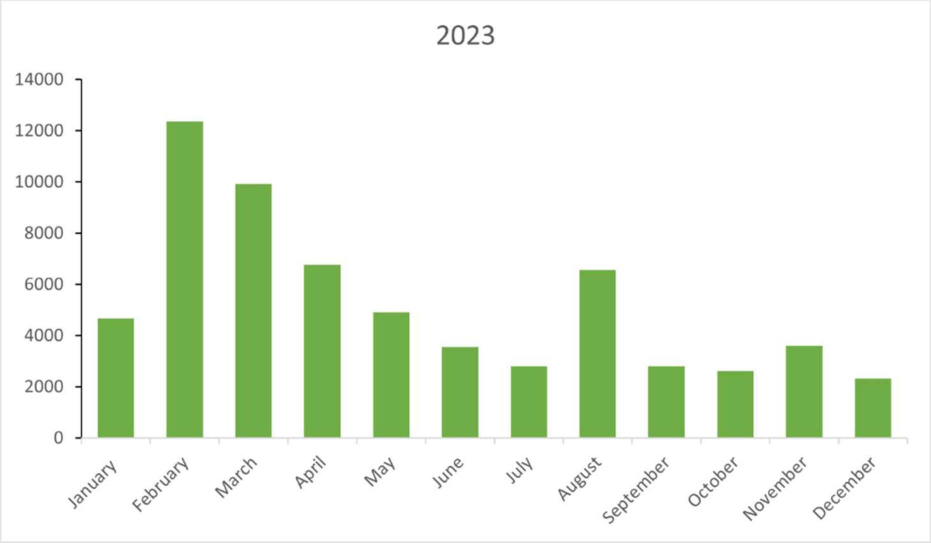


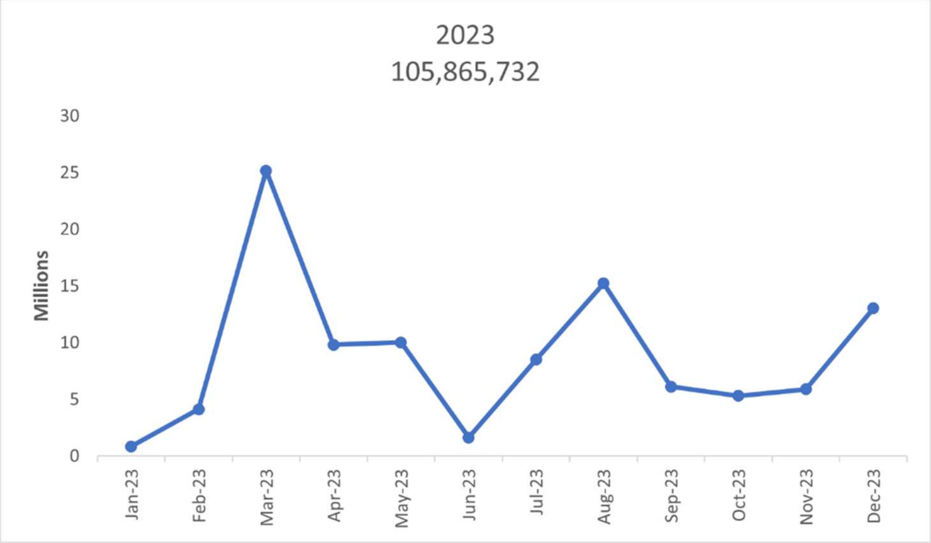
Figure 3. Malware Blocked



Cybersecurity Attacks

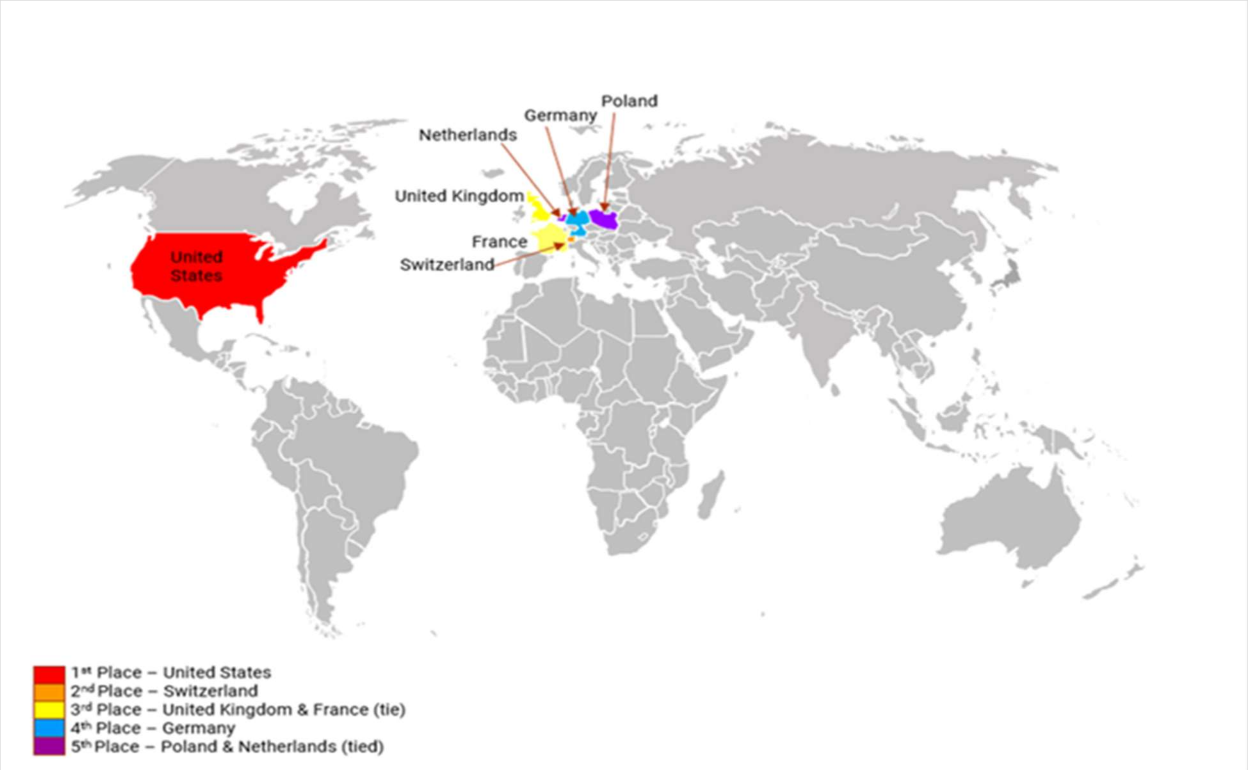
In 2023, 106 million attack attempts were detected against Commonwealth systems – a rate of 3.36 attacks every second. Spikes in activity often indicate new types of attack traffic. When an alert is triggered, traffic is analyzed to determine if it is malicious or authorized. Systems are then adjusted to prevent malicious attacks from penetrating the COV network. Alerts for known authorized traffic are fine-tuned to reduce false positives. The subsequent drop in attack attempts after a spike results from this system tuning.

Figure 4. Attack Attempts on COV Networks



In 2023, most attacks on the Commonwealth originated in the United States. The origins of the attacks on the Commonwealth's network are closely monitored and tracked. CSRM integrates threat intelligence from multiple sources into the security monitoring systems that protect Commonwealth data. This information is correlated with intelligence partners, enabling proactive blocking of attacks at their points of origin before systems are compromised. Over the past year, most attacks originate from within the United States, followed by Switzerland, the United Kingdom, France, Germany, Poland, and the Netherlands. However, it's important to note that the origin of an attack does not necessarily indicate its attribution. It's also important to note that the Commonwealth uses proactive geographical traffic controls to prevent interactions with hostile/hazardous parts of the world, which is why certain countries, such as China, Russia, and Ukraine are not represented in this data.

Figure 5. Top Five Attack Origins



Exploits and Vulnerabilities

In Q2 2023, CSRM introduced Acunetix 360. This cloud-based web scanning tool is used to detect and remediate web application vulnerabilities, thus reducing the risk of compromise to the Commonwealth's web presence. CSRM and agencies use this tool to scan websites for vulnerabilities and verify the success of remediation efforts. The tool provides agencies with online access to review scan results and retest vulnerabilities, which shortens remediation time and reduces risks.

Adoption of the tool allowed CSRM to increase scan frequency from a 90-day cycle in Q2 to a 30-day cycle by Q4. In 2023, 8,295 web scans were conducted, with 4,710 occurring in the last three months. These scans identified 610 critical and 1,745 high-severity vulnerabilities, of which 75% of critical and 69% of high-severity issues were resolved.

Vulnerabilities discovered by severity and month. Throughout the year, the number of critical and high-severity vulnerabilities fluctuated, with the highest discovery rates occurring in the first quarter as initial scans were conducted. After Q1, the number of newly identified vulnerabilities declined, but this trend reversed in Q4 due to an increase in monthly scans which included more internal dev/test sites. The number of scans rose from around 800 to approximately 2,000 per month in the final quarter. The increased scanning cadence ensures timely identification and a better chance of mitigation of security risks before they become problems.

The most common vulnerabilities fall into a few categories: Structured Query Language (SQL) injection, outdated technologies, and cross-site scripting.

Top Critical Vulnerabilities

Structured Query Language (SQL) Injection

SQL injection (SQLi): This vulnerability allows an attacker to access unauthorized data in a SQL database using dynamic queries and unvalidated user input. (Severity: Critical)

SQLi is a common attack vector that uses malicious SQL code to manipulate backend databases and access unintended information. This can include sensitive company data, user lists, or private customer details.

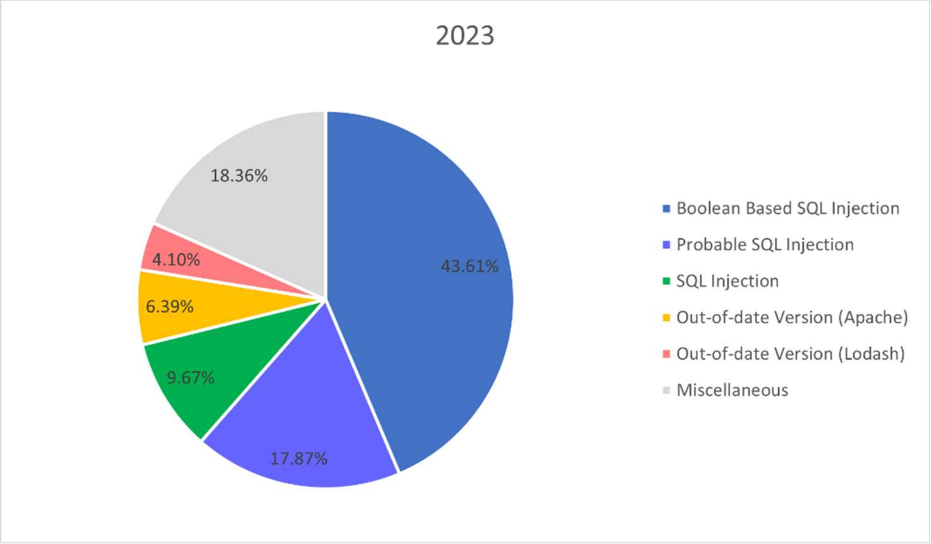
When an SQLi attack occurs, the vendor or developer must remediate the vulnerability, and database administrators must validate the database's data. In some cases, data breach notifications may also be required.

Outdated Technologies

This vulnerability occurs when a website uses technologies with known vulnerabilities. (Severity: Critical)

All websites rely on certain technologies for functionality. Over time, vulnerabilities in these technologies are discovered, and security patches are released. Failing to use the most up-to-date or secure versions leaves a website vulnerable to compromise. Strengthening web technology patching controls can help reduce exposure to such risks.

Figure 6. Top 5 Critical Web Vulnerabilities



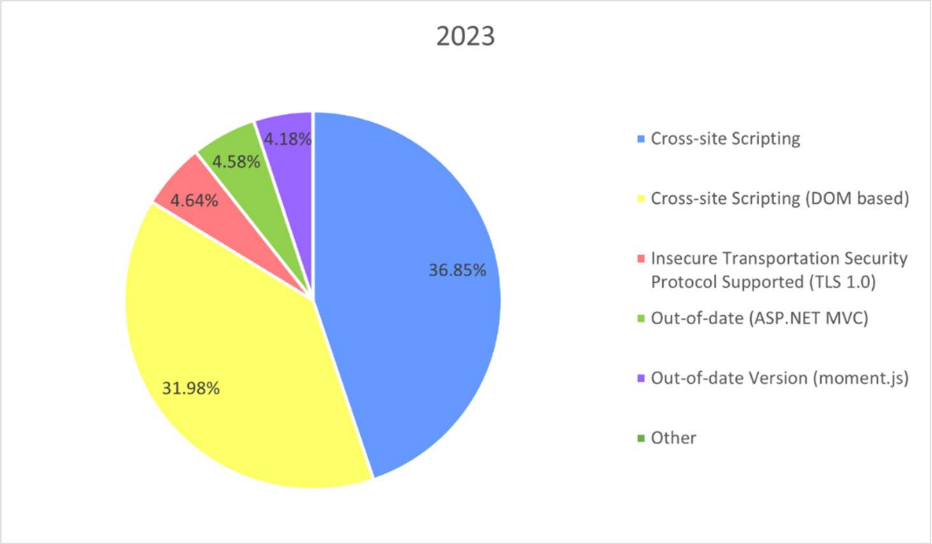
Top High Vulnerabilities

Cross-site scripting was the most prevalent of the top 5 high vulnerabilities.

Cross-site scripting (XSS) is a web application flaw that allows arbitrary JavaScript to be executed on a webpage. (Severity: High)

JavaScript is used in almost all websites to load and display various functionalities. XSS occurs when malicious JavaScript code, injected by an attacker, is loaded and executed in the user's browser due to poor input validation. This vulnerability can allow attackers to steal sensitive information, redirect users to malicious sites, or compromise user accounts.

Figure 7. Top 5 High Web Vulnerabilities



Security Investigations

The information received from Commonwealth partners, including state and local governments, higher education institutions, and public school systems, plays a critical role in enhancing security investigations by providing valuable data and insights needed to identify, analyze, and respond to potential threats across the Commonwealth. MS-ISAC compiles this data by monitoring the internet for potential incidents. CSRM disseminates alerts identified by the data to the affected entities and tracks them as investigations. Alerts are considered investigations until the results of the alerts are known.

Figure 8. Security Investigations by Entity

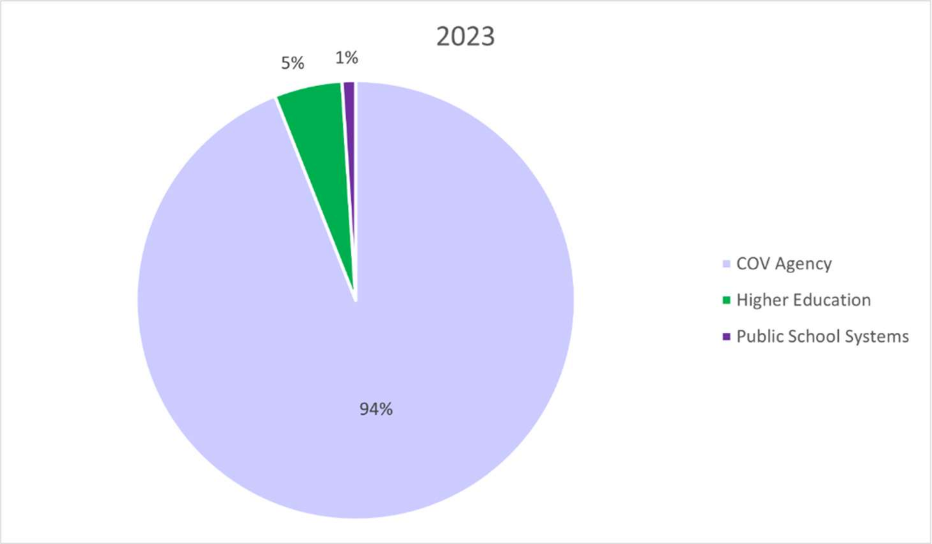
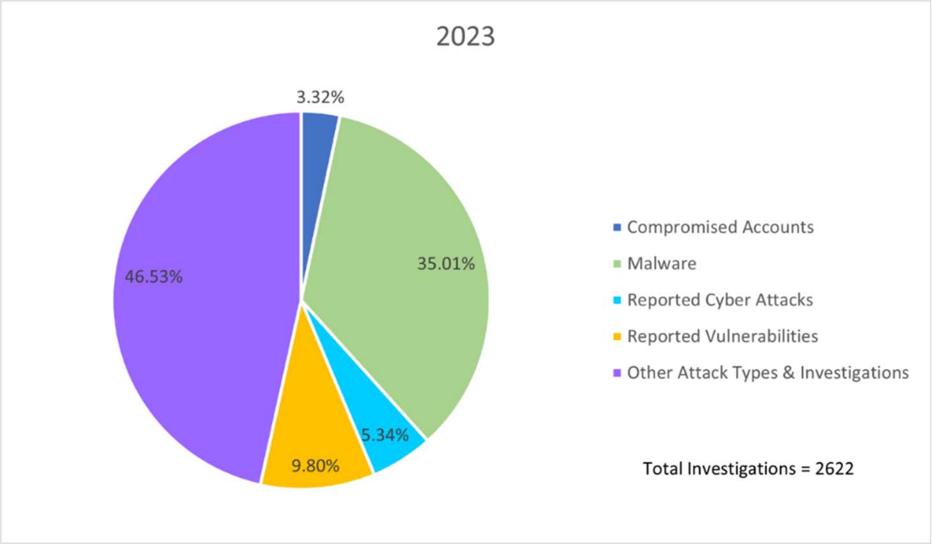


Figure 9. Security Investigations by Category



Commonwealth Information Security Program

The Commonwealth's information security governance program is responsible for monitoring performance and compliance against IT security policies and standards. It sets security strategy for the Commonwealth, supports agencies in their efforts to foster secure IT security environment, and promotes information security training and awareness.

Information Security Governance Program

Per § 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 accomplishes this undertaking by monitoring each agency's overall compliance with IT audit and information security risk program standards and policies.

In 2023, CSRM published Information Security Standard 530 aligning security controls with the National Institute of Standards and Technology (NIST) standard 800-53, Revision 5 and superseding information security standards 501 and 525 which were based on revision 4 of the controls document.

Security Awareness Training and Phishing Campaigns

In 2023, CSRM onboarded customer agencies to an enterprise-wide security awareness training platform.
User training is paramount to the protection of publicly owned assets. In 2023, VITA's security awareness training service was expanded to provide a centralized solution available to all of Commonwealth, not just executive branch agencies under VITA purview.
Using the latest threat intelligence, the CSRM Threat Management team designs campaigns to help Commonwealth users recognize common phishing attacks.

CSRM has developed a free simulated phishing service to supplement security awareness training. These campaigns reinforce security awareness training and allow users to practice their skills in a safe environment.

ISO Orientation and Certification

CSRM provides an introductory and recertification training course for Commonwealth information security officers (ISOs).

The course provides an overview the Commonwealth's information security program, processes, services, and CSRM contact information. In 2023, 118 attendees completed the virtual course. The course schedule is posted on VITA website with a registration form. CSRM recommends ISOs attend a session at the earliest opportunity after assuming the ISO role and responsibilities.

Information Security Officer Advisory Group (ISOAG)

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 improve the security posture of the Commonwealth through the exchange of IT security knowledge. Every year, CSRM conducts monthly meetings with knowledgeable speakers from government and private sector organizations to share their information security expertise at no cost to attendees.

Meeting attendance allows members to earn continuing professional education credits (CPE), a requirement necessary for security professionals to maintain their security certifications and memberships in global security organizations. It also provides an opportunity to share best practices, allow feedback on proposed policy changes and receive information concerning local training opportunities. Meeting presentation materials are posted to the VITA website as an additional resource to the group. In 2023, the ISOAG average attendance count was 200.

Commonwealth Security Information Council (CISC)

A select group of information security officers from various state agencies, with support of CSRM, comprise the Commonwealth IS Council.

The IS Council recommends strategic direction for information security and privacy initiatives in the Commonwealth. The purpose of the council is to increase, through education, the understanding of key business processes of state agencies; to obtain consensus and support for enterprise-wide IT security initiatives; to identify key areas for process improvement; and to coordinate agency business processes with VITA's processes. CSRM will continue to engage with the IS Council to obtain agency input on practical and effective security initiatives.

IT Risk Management Committee

The IT Risk Management Committee is made up of risk specialists from CSRM's IT Risk Management division and information security officers from other Commonwealth agencies.

The committee meets monthly to discuss approaches to addressing risks and issues identified as significant. In addition, the committee determines the prioritization of risk mitigation as well as provides feedback on the current approaches to maintain established risk thresholds. The committee documents and reports risk alerts to escalate issues with potential significant impact to the enterprise or customer agencies. As a result, VITA, agencies, and the associated service providers have made significant progress in the mitigation of the potential threats and impacts of the risk and issues identified.

Third-Party Risk Management

CSRM has developed and implemented methodologies for monitoring and managing risks associated with third-party service providers.

The amount of risk introduced by third parties is quantified to ensure the Commonwealth maintains established risk thresholds. CSRM also plays an integral role in the multisourcing services integrator (MSI) model to identify cybersecurity risks and track through resolution. As a result, VITA and the associated service providers have addressed IT security threats before there was significant impact to COV data and systems.

Commonwealth agencies' need for Cloud Services continues to increase.

In response to increased cloud adoption, CSRM established a security review process for third-party systems and services to ensure those services are secure, dependable and resilient. The COV Ramp service, formerly known as Enterprise Cloud Oversight Service (ECOS), is a service specifically created for establishing contract terms and oversight of third-party vendors offering Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) applications. SaaS is a type of cloud service where an application runs on infrastructure not owned or managed by the

Commonwealth. CSRM provides pre-contracting assessment of systems to ensure the appropriate controls are in place prior to being implemented.

Table 1. 2017-2023 COV Ramp Assessments

COV Ramp	2017	2018	2019	2020	2021	2022	2023
# of Assessments by Date Submitted	75	89	82	70	148	100	136
# of Assessments by Date Completed	24	68	76	53	101	86	123
Avg Entering Active Oversight	17	48	53	37	71	60	86
Avg Cumulative Total Oversight	17	65	118	155	226	286	372

Centralized Shared Security Services

To supplement agency IT security programs, CSRM offers centralized shared services. These services include IT security auditing, ISO support, and web application vulnerability scanning programs. IT security auditing and ISO support services are optional programs that agencies can acquire based on their security needs. Web application vulnerability scanning is a mandatory program that identifies potential weaknesses in agency websites and recommends actions to address concerns identified in the scans. All these services enhance information security and compliance in the Commonwealth.

IT Audit Service

In the past, many agencies did not perform required IT security audits because they did not have their own IT auditing departments or otherwise did not have funds to hire outside auditing resources. The centralized IT auditing service assists these agencies with documenting their IT security audit plans, conducting IT security audits, and supporting agency efforts to create and submit corrective action plans to address the issues found during audits. Currently 34 agencies have elected to use the shared centralized audit service to perform IT security audits.

Shared ISO Service

In 2023, 37 customer agencies subscribed to the ISO service. The shared ISO service helps agencies maintain their key IT risk management tools, including business impact analysis (BIA), risk assessment plans, and IT system risk assessments.

Web Application Vulnerability Scanning

Automated scans of Commonwealth public-facing websites identify potential security weaknesses that the agencies can address to prevent attacks. CSRM scans over 6,000 public sites (targets) every quarter. Additionally, CSRM scans private sensitive sites with operating system level scans and application-level sites for sensitive applications. In 2023, CSRM released new security tools improving web application vulnerability scanning processes for information security officers.

IT Audit & IT Risk Compliance

CSRM monitors information security programs to ensure minimum IT audit and IT risk management functions are completed.

Per §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 accomplishes this undertaking by monitoring each agency's overall compliance with IT audit and information security risk program standards and policies.

The IT audit and IT risk compliance processes use pre-defined metrics to measure compliance each calendar year.

Using a 10-point grading scale, program scores are converted into letter grades: A, B, C, D, E, and F. The compliance grade provides a familiar measurement tool to reflect the degree to which agencies are completing their necessary IT security requirements. In addition, the compliance grades clearly identify agency IT strengths and opportunities for improvement.

The Commonwealth IT audit compliance program includes review and oversight of the agency's IT auditing activities, including submission of audit plans, completed audits and corrective actions.

The completion of these items determines an agency's overall audit program score.
The audit compliance score is based on an agency submission of an IT security audit plan, agency submission of quarterly updates to their IT security audit findings, and completion of required IT security audits.

The Commonwealth IT risk management program entails the review and oversight of agencies' IT risk management activities.

The program requires the submission of agency data sets, business impact analysis (BIA), risk assessment plans, risk assessments, risk findings updates, ISO certification/reporting and intrusion detection reports. These submitted and approved pieces of data represent the components used to determine the agencies' overall risk program score. The risk compliance grades reflect the varying maturity of risk management programs at the agencies.

2023 IT Audit and Risk Compliance and Grades

In 2023, 44% of IT audit compliance grades were above average.

Overall audit compliance grades improved by 8% in 2023. CSRM recommends that agencies continue to complete required audits, audit plans, and provide quarterly findings updates.

In 2023, 74% of IT risk compliance grades were above average.

Overall IT risk compliance increased 27% in 2023. Multiple risk metrics increased to include quarterly finding updates and completion of required risk assessments. CSRM recommends that agencies continue to satisfy risk management requirements.

Figure 10. 2020 - 2023 Audit Compliance Grades

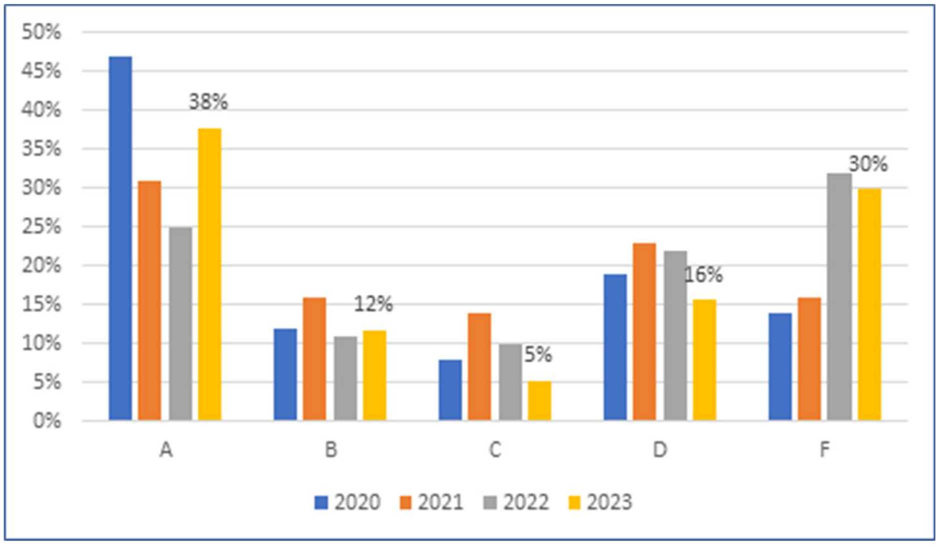


Figure 11. 2020 - 2023 Risk Compliance Grades

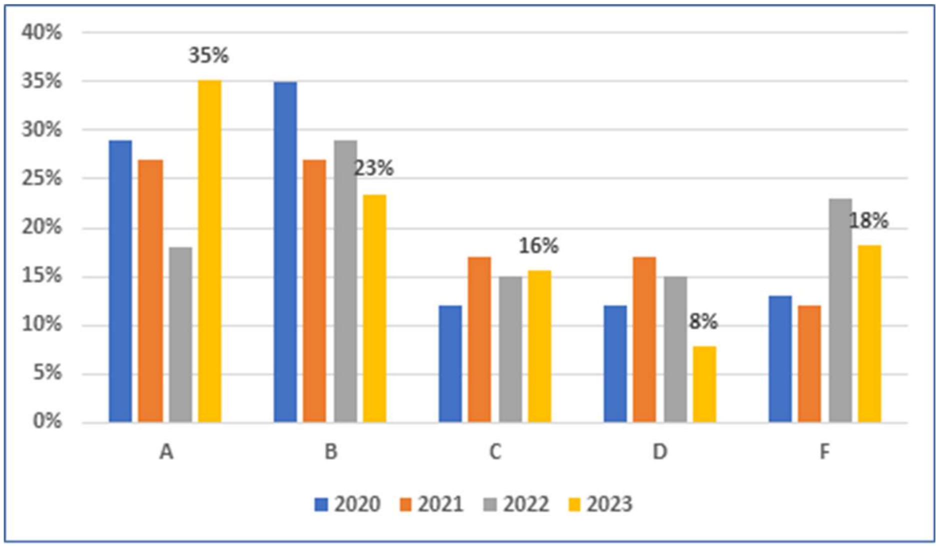


Figure 12. 2023 IT Audit & Risk Compliance Analysis

2023 IT Audit & Risk Compliance Analysis				
Program	**Metric**	**Full Compliance Rate**	**1 Year Change**	**Notes**
Audit	Audit Plan	82%	Same	
	Three-Year Audit Obligation	29%	11% Decrease	40% partial compliance
	Current Year Percentage of Quarterly Findings Updates Received: Audit	57%	4% Decrease	30% partial compliance
Risk	Risk Assessment Plan	75%	No change	
	Three-Year IT Risk Assessment Obligation	27%	14% Increase	30% partial compliance
	Business Impact Analysis	62%	18% Decrease	8% partial compliance
	(BIA) Status			
	Current Year Percentage of Quarterly Findings Updates Received: IT risk assessments	66%	28% Increase	27% partial compliance
	Quarterly Intrusion Detection Systems (IDS) reports are received	94%	3% Increase	
	Applications Certified	90%	3% Increase	3% partial compliance
	ISO Certification Status	86%	8% Increase	
	ISO Reports to Agency Head	84%	3% Increase	

IT Audit and IT Risk Findings

CRSM's risk management team also monitors the progress and remediation of IT audit and risk findings. IT audit and IT risk assessment findings identify specific gaps with security controls. An IT audit finding identifies a compliance gap, whereas a risk finding includes threat and business impact analysis to determine potential harm or loss as result of the gap.

In 2023, CSRM reports the average age for all open IT audit and risk findings is 948 and 1,313 days respectively. To reduce risk, CSRM recommends agencies use mitigating controls until findings can be remediated. CSRM also recommends agencies conduct regular review of findings to assess the effectiveness of mitigating controls and risk is being managed as expected.

Combined, 33% of audit and risk findings are related to security controls used to manage access to Commonwealth information. Common findings in this area include lack of appropriate policy and/or procedures for the authorization and approval of access, lack of routine reviews of accounts and access granted to information. CSRM recommends agency document access control policies, develop and adhere to regular review of accounts and privileges to reduce the impact of unauthorized use or disclosure of Commonwealth information.

Figure 13. 2023 Findings by Secretariat

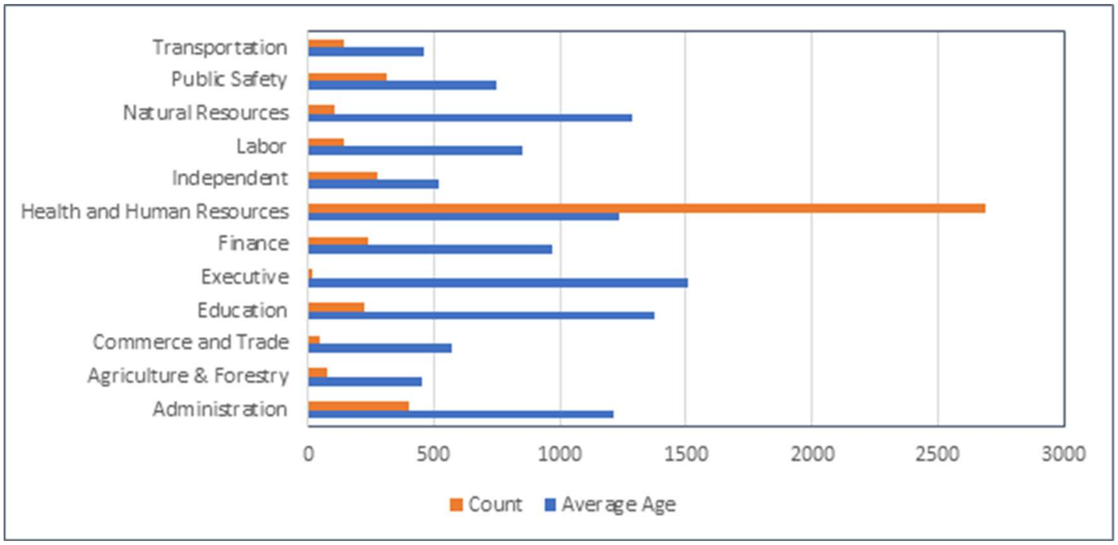
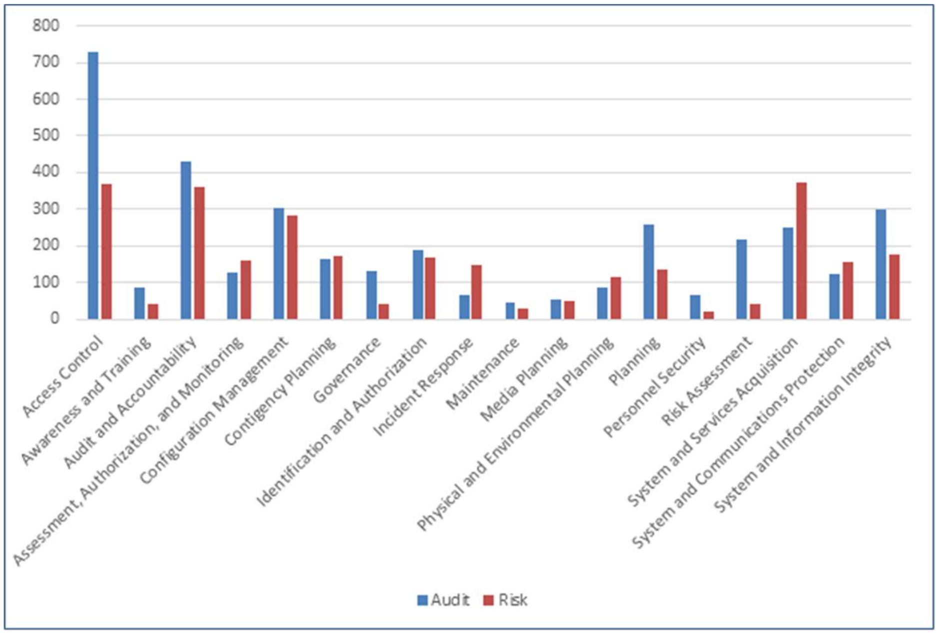


Figure 14. Audit and Risk Findings by Security Control Family



Nationwide Cybersecurity Review (NCSR) Assessment

NCSR Assessment Background

Annually, the Commonwealth participates in the National Cyber Security Review (NCSR) sponsored by the Multi-State Information Sharing & Analysis Center (MS-ISAC). The NCSR is a self-assessment survey aligned within the NIST cybersecurity framework (CSF) to evaluate an agency's cybersecurity posture. Nationally the survey has a very high participation rate, and the cumulated results are reported biannually to the US Congress.

The NCSR provides significant insight into IT security practice at each agency by identifying gaps in performance areas that allow us to benchmark year-to-year progress. In addition, the review provides a way to measure and compare the Commonwealth against other peer survey participants across the nation.

Each agency participating in the survey, ranks their performance on a maturity scale for five core cybersecurity functions: *identify, protect, detect, respond and recover*. The maturity scale goes from a low score of one (activity is not performed, i.e., no processes, policies or technologies are in place) to a high score of seven (activity is optimized, i.e., policies and procedures are formally documented, implemented, tested, and continuously monitored for effectiveness). NCSR recommends a minimum maturity level score of five.

2023 Assessment Survey

In 2023, 48 states participated in the NCSR assessment including 25 Commonwealth agencies. The Commonwealth reports slightly higher scores than peer states, continues to trend higher in the identify and protect functional areas, and reports more conservative scores in the detect and respond function. Agencies, nationally and in the Commonwealth, providing information technology or financial services report higher than average maturity scores. Agencies supporting elections and education sub sectors report maturity levels slightly below average. CSRM recommends Commonwealth agencies continue to participate in the assessment to identify opportunities to improve information security programs and security services.

Peer Assessment

In 2023, the average maturity score for CSF functions for the Commonwealth is 5.47 (on a 7-point scale), down from 5.49 in 2022.

The overall average for participating states submissions also declined slightly from 5.08 to 4.99. MS-ISAC grouped all nationally participating agencies into peer group subsectors by government service/business function. CSRM combined COV agencies into similar subsectors groups to compare. Functionally, participating Commonwealth agencies rank themselves more mature in the identity and protect functions with lower maturity in the detect, respond, and recover functions. Commonwealth agencies report higher maturity levels than peer states and sub sectors. CSRM recommends Commonwealth agencies continue to monitor maturity levels and execute improvement plans.

Figure 15. 2023 Commonwealth (COV) averages compared to other state agencies and states

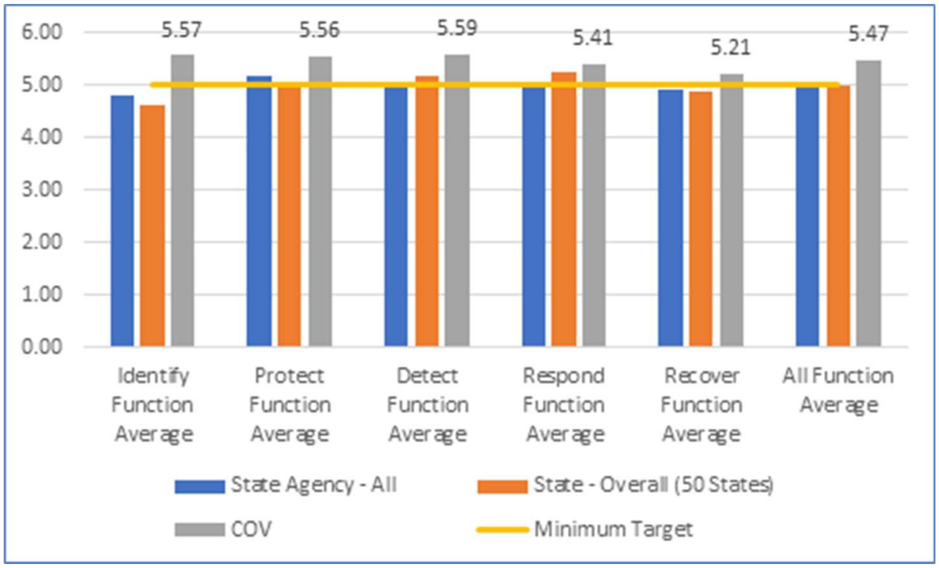


Figure 16. 2023 Commonwealth (COV) Identify function peer assessments by sub sector

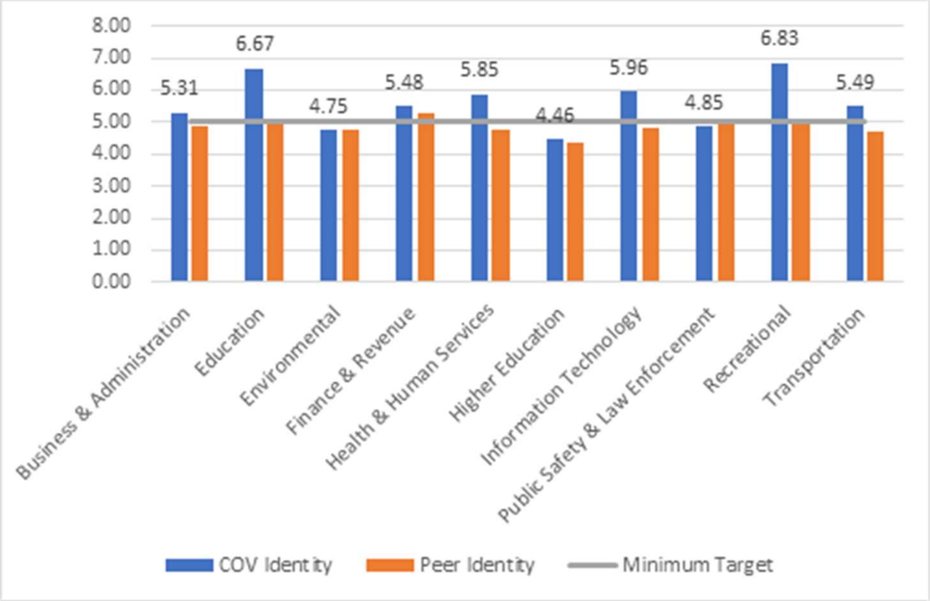


Figure 17. 2023 Commonwealth (COV) Protect function peer assessments by sub sector

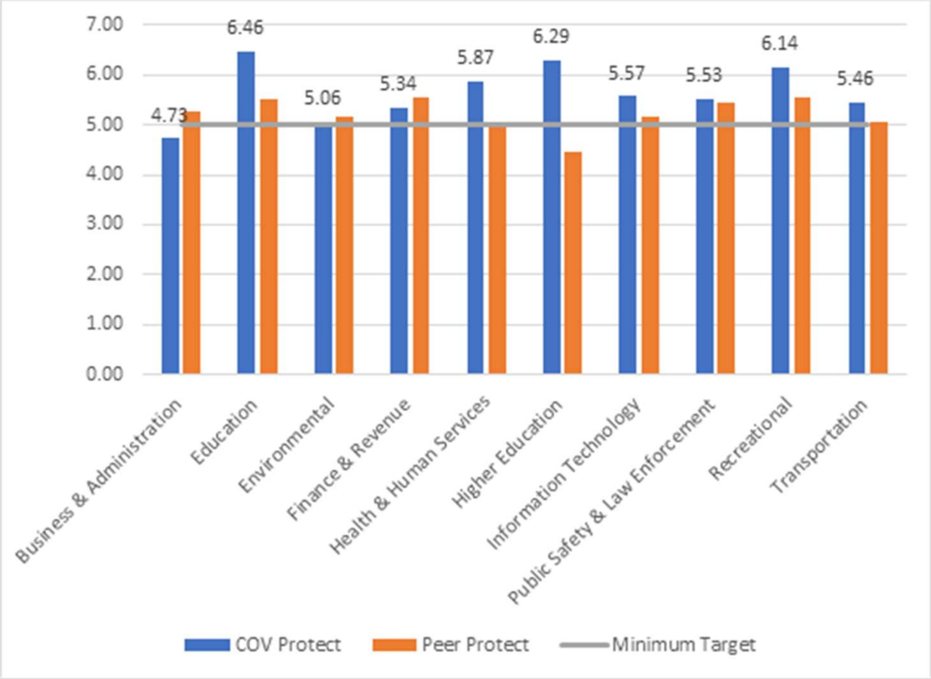


Figure 18. 2023 Commonwealth (COV) Detect function peer assessment by sub sector

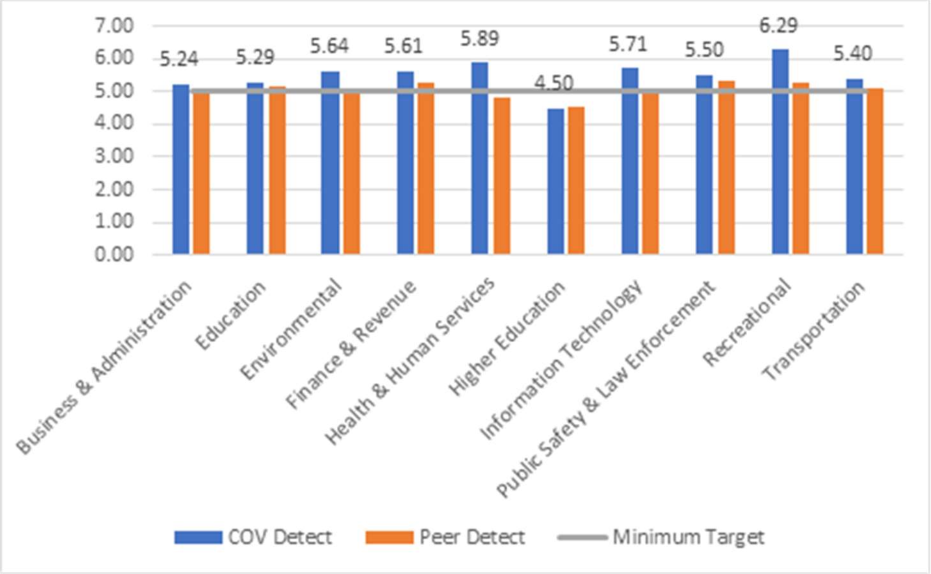


Figure 19. 2023 Commonwealth (COV) Respond function peer assessment by sub sector

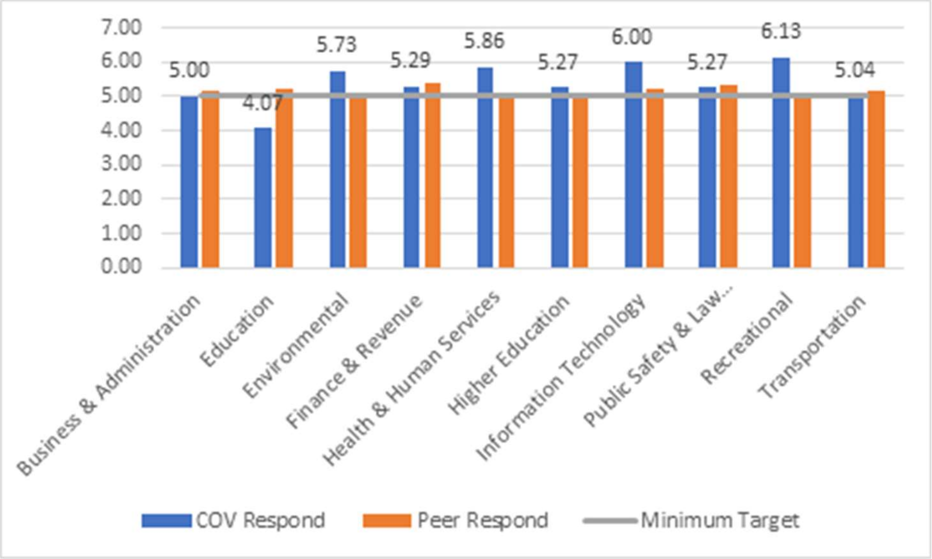
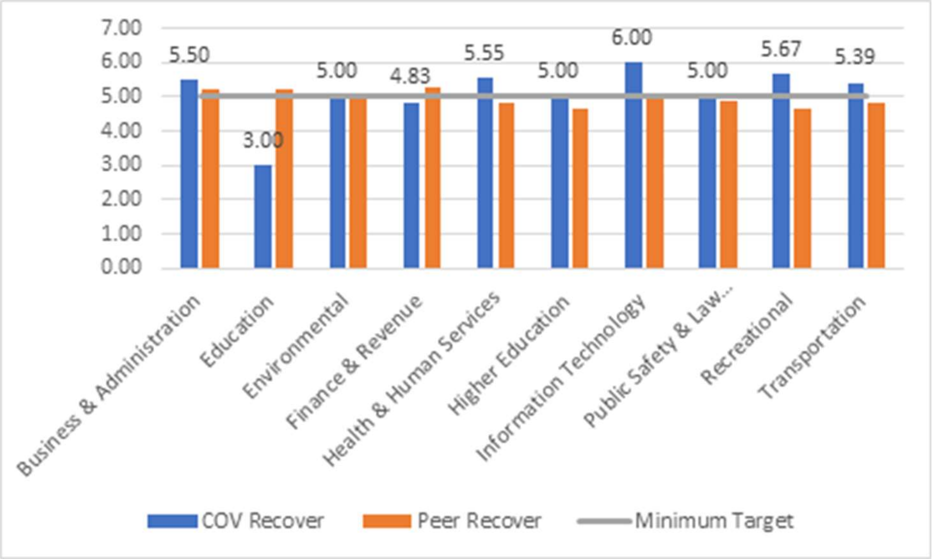


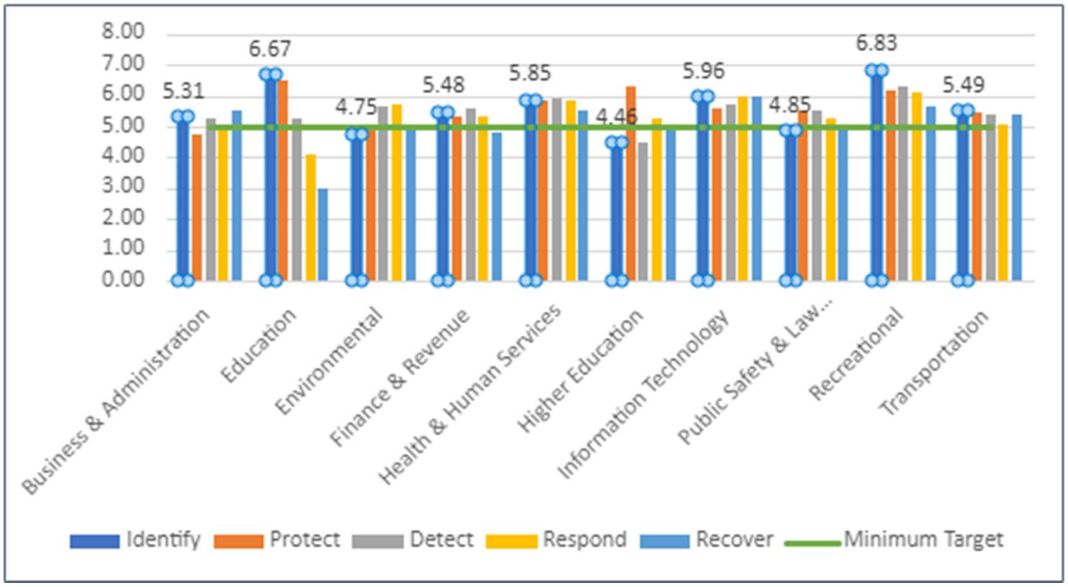
Figure 20. 2023 Commonwealth (COV) Recover function peer assessment by sub sector



Commonwealth Self-Assessment

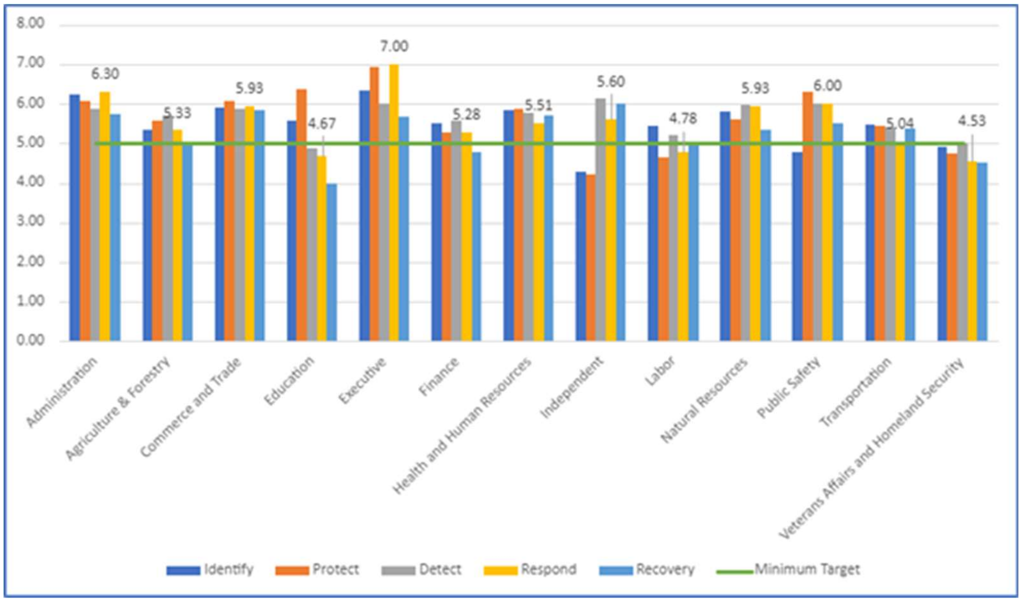
In 2023, the Commonwealth's information technology and recreational subsectors report higher maturity scores in all functions. Commonwealth education and higher education organizations report lower maturity scores. Commonwealth education organization report higher maturity in the identify and protect functions but significantly lower maturity levels in the respond and recover functions.

Figure 21. 2023 Commonwealth (COV) Functional self-assessment by sub sector



Most Commonwealth secretariats report at least one functional area meeting the recommended maturity level of 5. Overall, agencies continue to report lower scores in the Detect, Respond, and Recovery functions.

Figure 22. 2023 Commonwealth (COV) Functional self-assessment by secretariat



Commonwealth agencies continue to report higher scores in the overall Protect function metric, a consistent trend since 2019. Overall scores in the Detect and Respond function continue to trend lower for Commonwealth agencies. In 2023, Commonwealth category averages ranged from 5.20 to 5.84.

Table 2. 2023 NCSR Self-Scoring Results

Function	Categories	COV Averages
Identify	Asset Management	5.68
	Business Environment	5.54
	Governance	5.77
	Risk Assessment	5.54
	Risk Management Strategy	5.16
Protect	Access Control	5.78
	Awareness and Training	5.72
	Data Security	5.66
	Information Protection Processes and Procedures	5.42
	Maintenance	5.66
	Protective Technology	5.28
Detect	Anomalies and Events	5.35
	Continuous Monitoring	5.7
	Detection Processes	5.84
Respond	Analysis	5.49
	Communications	5.3
	Improvements	5.28
	Mitigation	5.5
	Response Planning	5.56
Recover	Communications	5.21
	Improvements	5.22
	Recovery Planning	5.2

Appendix I. Agency Information Security Data Points

Legend

Audit plan status
Pass - Documents received as scheduled
Non-compliant (N/C) - Missing audit plan

Percentage of audit findings updates received
X% - The percentage of due findings updates received
N/A - Not applicable as the agency had no updates due

Three-year audit obligation
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 current security audit plan

Risk assessment plan status
Pass - Documents received as scheduled
N/C - Missing risk assessment plan

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 risk assessment plan

Percentage of risk findings updates received
X% - The percentage of due risk findings updates received
N/A - Not applicable as the agency had no risk updates due

Business Impact Analysis status
N/C – the data provided is incomplete, and there is an active application without any business processes
X% – The percentage of business processes that have been submitted and approved within the last 365 days

Intrusion Detection System (IDS) quarterly reports
Pass - Documents received as scheduled
N/C - Reports were not received

Applications Certified
Compliant – Agency application inventory is compliant for completeness
N/C – Agency application inventory is incomplete

ISO certification status
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

ISO reports to Agency Head
Yes - Agency ISO reports to Agency Head
No - Agency ISO does not report directly to Agency Head

Agency Secretariat	Agency Name	Audit Plan Status	Percentage of Audit Finding Updates Received	Three-Year Audit Obligation	Risk Assessment Plan Status	Three- Year Risk Assessment Obligation	Percentage of Risk Finding Updates Received	Business Impact Analysis Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head
Administration	Compensation Board	Pass	N/A	N/C	Pass	0%	N/A	43%	Pass	Compliant	Pass	Yes
Administration	Department of Elections	Pass	0%	100%	Pass	100%	50%	100%	Pass	Compliant	Pass	Yes
Administration	Department of General Services	Pass	0%	0%	N/C	N/C	0%	N/C	Pass	Compliant	Pass	Yes
Administration	Department of Human Resource Management	Pass	100%	83%	Pass	75%	80%	100%	Pass	Compliant	Pass	Yes
Administration	Office of Data Governance and Analytics	Pass	N/A	N/A	Pass	N/A	100%	100%	Pass	Compliant	Pass	Yes
Administration	Virginia Information Technologies Agency	Pass	20%	63%	Pass	N/C	58%	97%	Pass	Compliant	Pass	Yes
Agriculture & Forestry	Department of Forestry	Pass	100%	100%	Pass	33%	100%	100%	Pass	Compliant	Pass	No
Agriculture & Forestry	Virginia Department of Agriculture and Consumer Services	Pass	100%	100%	Pass	43%	72%	100%	Pass	Compliant	Pass	Yes
Agriculture & Forestry	Virginia Racing Commission	Pass	96%	33%	N/C	N/C	44%	100%	Pass	Compliant	Pass	Yes
Commerce and Trade	Board of Accountancy	Pass	N/A	0%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes
Commerce and Trade	Department of Housing and Community Development	Pass	100%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Commerce and Trade	Department of Small Business	Pass	86%	75%	Pass	75%	100%	100%	Pass	Compliant	Pass	Yes

	and Supplier Diversity											
Commerce and Trade	Tobacco Region Revitalization Commission	N/C	N/A	N/C	N/C	N/C	N/A	0%	Pass	Compliant	N/C	Yes
Commerce and Trade	Virginia Economic Development Partnership	N/C	N/A	N/C	N/C	N/C	N/A	N/C	Fail	Non-Compliant	Pass	No
Commerce and Trade	Virginia Employment Commission	Pass	8%	14%	Pass	63%	95%	100%	Pass	Compliant	Pass	Yes
Commerce and Trade	Virginia Energy	Pass	0%	100%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes
Commerce and Trade	Virginia Innovation Partnership Corporation	Pass	N/A	78%	Pass	100%	N/A	100%	Pass	Compliant	N/C	Yes
Education	Department of Education	Pass	84%	71%	Pass	71%	100%	N/C	Pass	Compliant	Pass	Yes
Education	Frontier Culture Museum of Virginia	Pass	N/A	0%	Pass	50%	N/A	100%	Pass	Compliant	Pass	Yes
Education	Gunston Hall	Pass	0%	N/C	Pass	0%	0%	100%	Pass	Compliant	Pass	Yes
Education	Jamestown-Yorktown Foundation	N/C	0%	77%	N/C	N/C	0%	N/C	Pass	Compliant	N/C	No
Education	Library of Virginia	Pass	100%	6%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes
Education	New College Institute	N/C	N/A	N/C	N/C	N/C	N/A	0%	Fail	Non-Compliant	N/C	Yes
Education	Richard Bland College	Pass	40%	0%	Pass	N/C	N/A	100%	Fail	Compliant	Pass	Yes
Education	Science Museum of Virginia	N/C	N/A	N/C	N/C	N/C	0%	0%	Pass	Compliant	N/C	Yes
Education	Southern Virginia Higher Education Center	Pass	N/A	N/A	Pass	N/A	N/A	100%	Pass	Compliant	Pass	No
Education	Southwest Virginia Higher Education Center	N/C	N/A	N/C	N/C	N/C	N/A	0%	Fail	Non-Compliant	N/C	No

Education	State Council of Higher Education for Virginia	Pass	2%	0%	Pass	0%	3%	0%	Pass	Compliant	Pass	Yes
Education	Virginia Commission for the Arts	Pass	N/A	0%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes
Education	Virginia Museum of Fine Arts	Pass	67%	100%	Pass	100%	0%	0%	Pass	Compliant	Pass	Yes
Education	Virginia School for the Deaf and Blind	N/C	N/A	N/C	N/C	N/C	N/A	0%	Fail	Compliant	N/C	Yes
Education	Virginia State University	Pass	0%	100%	N/C	N/C	N/A	0%	Pass	Compliant	Pass	Yes
Executive	Office of Attorney General	N/C	0%	N/C	N/C	N/C	N/A	N/C	Pass	Non-Compliant	Pass	No
Executive	Office of State Inspector General	Pass	100%	100%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes
Executive	Office of the Governor	Pass	N/A	N/A	Pass	N/A	100%	N/C	Pass	Compliant	Pass	Yes
Finance	Department of Accounts	Pass	100%	96%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes
Finance	Department of Planning and Budget	Pass	58%	83%	N/C	N/C	6%	12%	Pass	Compliant	Pass	Yes
Finance	Department of Taxation	Pass	99%	79%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Finance	Department of Treasury	Pass	20%	21%	Pass	100%	90%	100%	Pass	Compliant	Pass	Yes
Health and Human Resources	Department for Aging and Rehabilitative Services	Pass	80%	80%	Pass	20%	95%	100%	Pass	Compliant	Pass	Yes
Health and Human Resources	Department for the Deaf and Hard of Hearing	Pass	N/A	100%	Pass	100%	100%	100%	Pass	Partial	Pass	Yes
Health and Human Resources	Department of Behavioral Health and Development Services	Pass	92%	N/C	N/C	N/C	100%	N/C	Pass	Compliant	Pass	Yes
Health and Human Resources	Department of Health Professions	Pass	N/A	100%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes

Health and Human Resources	Department of Medical Assistance Services	Pass	100%	98%	Pass	45%	73%	N/C	Pass	Compliant	Pass	Yes
Health and Human Resources	Department of Social Services	Pass	0%	18%	N/C	N/C	40%	N/C	Pass	Compliant	Pass	Yes
Health and Human Resources	Office for Children's Services	Pass	100%	71%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Health and Human Resources	Virginia Department of Health	Pass	98%	55%	Pass	17%	99%	100%	Pass	Compliant	Pass	Yes
Health and Human Resources	Virginia Foundation for Healthy Youth	N/C	N/A	N/C	N/C	N/C	N/A	N/C	Pass	Non-Compliant	N/C	Yes
Independent	Indigent Defense Commission	Pass	50%	25%	Pass	100%	89%	100%	Pass	Compliant	Pass	Yes
Independent	State Corporation Commission	Pass	98%	79%	Pass	92%	56%	100%	Pass	Compliant	Pass	Yes
Independent	State Lottery Department	Pass	100%	80%	Pass	40%	N/A	100%	Pass	Compliant	Pass	Yes
Independent	Virginia College Savings Plan	N/C	0%	N/C	N/C	N/C	N/A	0%	Pass	Non-Compliant	Pass	Yes
Independent	Virginia Retirement System	Pass	100%	95%	Pass	80%	92%	100%	Pass	Compliant	N/C	Yes
Independent	Virginia Workers Compensation Commission	Pass	N/A	100%	Pass	73%	N/A	100%	Pass	Compliant	Pass	Yes
Labor	Department of Labor and Industry	Pass	56%	100%	Pass	86%	N/A	100%	Pass	Compliant	Pass	Yes
Labor	Department of Professional and Occupational Regulation	Pass	N/A	75%	Pass	75%	100%	100%	Pass	Compliant	Pass	Yes
Natural Resources	Department of Conservation and Recreation	Pass	N/A	100%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes

Natural Resources	Department of Environmental Quality	Pass	45%	36%	Pass	7%	25%	35%	Pass	Compliant	Pass	Yes
Natural Resources	Department of Historic Resources	Pass	100%	N/A	N/C	N/C	N/A	100%	Pass	Compliant	Pass	Yes
Natural Resources	Department of Wildlife Resources	N/C	4%	N/C	Pass	0%	N/A	N/C	Pass	Compliant	Pass	No
Natural Resources	Marine Resources Commission	Pass	83%	100%	Pass	100%	100%	N/C	Pass	Compliant	Pass	Yes
Natural Resources	Virginia Museum of Natural History	Pass	100%	N/A	Pass	N/A	100%	100%	Pass	Compliant	Pass	Yes
Public Safety	Commonwealths Attorneys Services Council	Pass	N/A	N/A	Pass	N/A	N/A	100%	Pass	Compliant	Pass	Yes
Public Safety	Department of Corrections	Pass	74%	100%	Pass	83%	75%	100%	Pass	Compliant	Pass	Yes
Public Safety	Department of Criminal Justice Services	Pass	100%	66%	Pass	62%	100%	100%	Pass	Compliant	Pass	Yes
Public Safety	Department of Fire Programs	N/C	N/A	N/C	Pass	86%	N/A	100%	Pass	Compliant	N/C	No
Public Safety	Department of Forensic Science	Pass	100%	100%	Pass	100%	25%	100%	Pass	Compliant	Pass	Yes
Public Safety	Department of Juvenile Justice	N/C	0%	N/C	N/C	N/C	N/A	95%	Pass	Partial	Pass	Yes
Public Safety	Department of Military Affairs	N/C	N/A	N/C	Pass	N/C	N/A	N/C	Pass	Compliant	N/C	No
Public Safety	Department of Veterans Services	Pass	100%	33%	Pass	0%	N/A	N/C	Pass	Compliant	Pass	Yes
Public Safety	Virginia Department of Emergency Management	Pass	N/A	N/C	Pass	0%	N/A	96%	Pass	Compliant	Pass	Yes
Public Safety	Virginia State Police	Pass	67%	64%	N/C	N/C	N/A	100%	Pass	Compliant	Pass	Yes

Transportation	Department of Aviation	Pass	100%	66%	Pass	67%	50%	100%	Pass	Compliant	Pass	Yes
Transportation	Department of Motor Vehicles	Pass	100%	25%	Pass	79%	100%	100%	Pass	Compliant	Pass	Yes
Transportation	Department of Rail and Public Transportation	Pass	N/A	100%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes
Transportation	Motor Vehicle Dealer Board	Pass	25%	50%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes
Transportation	Virginia Department of Transportation	Pass	100%	79%	Pass	25%	92%	100%	Pass	Compliant	Pass	No

[1]

[1] In 2023, 77 organizations were in scope to the annual compliance report.

Appendix II. Information Security Program Metrics

Program	Metric	Description
IT Audit	Audit Plan	Identifies system & calendar year an audit will be performed per triennial requirements for sensitive systems
	Three-Year Audit Obligation	Percentage of sensitive systems with complete audits satisfying the triennial requirement
	Current Year Percentage of Quarterly Findings Updates Received: Audit	Percentage of quarterly updates received compared to number open audit findings
IT Risk Management	Risk Assessment Plan	Identifies IT system & year a risk assessment will be completed per triennial requirements for sensitive systems
	Three-Year IT Risk Assessment Obligation	Percentage of complete IT risk assessments compared to the triennial requirement

		for sensitive systems
	Business Impact Analysis (BIA) Status	Business processes are identified and aligned with IT assets, business impact areas are quantified, and sensitivity classifications are identified
	Current Year Percentage of Quarterly Findings Updates Received: IT risk assessments	Percentage of quarterly updates received compared to number open IT risk assessment findings
	Quarterly Intrusion Detection Systems (IDS) reports are received	Quarterly Intrusion Detection Systems (IDS) reports are received. *No action required if in COV infrastructure*
	Applications Certified	Minimum information for each application is recorded
	ISO Certification Status	Primary ISO satisfies all certification requirements
	ISO Reports to Agency Head	Organization structure confirms ISO reports to the Agency Head

Appendix III. NCSR Self-Assessment Standards

- ***Identify:*** The activities measured for this function are key for an agency's understanding of their internal culture, infrastructure and risk tolerance.
    - "Asset Management" is the data, personnel, devices, system, and facilities that enable the organization to achieve business purposes. Assets must be identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
    - The "Business Environment" category is related to how the organization's missions, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
    - "Governance" is related to how the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
    - "Risk Assessment" describes how the organization understands the cybersecurity risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
    - "Risk Management Strategy," the least mature category in the identify function, describes how the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. This may indicate that additional resources to assist with formal risk management assessments could be beneficial to Commonwealth agencies.
    - Lastly, "Supply Chain Risk Management" relates to how the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support supply chain decisions.
- ***Protect*:** The activities under the protect function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services.
    - "Access Control" describes how access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
    - "Awareness and Training" designates how the organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security related duties and responsibilities.
    - "Data Security," the most mature category in this function, refers to the idea that information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

  - "Information Protection Processes and Procedures" describes how the security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
  - "Maintenance" is related to the maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
  - "Protective technology," which refers to the technical security solutions that are used to manage the security and resilience of systems and assets and their consistency with related policies, is the least mature category in the protect function. This specifies that agencies may need more guidance regarding best practices for ensuring that technical security solutions are managed correctly.
- ***Detect:*** The quicker an agency is able to detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the detect function pertain to an organization's ability to identify incidents.
  - "Anomalies and Events" measures capabilities related to detecting anomalous activity and understanding the potential impact of events that are detected.
  - "Continuous Monitoring" measures the capability to monitor systems and assets to identify cybersecurity events and verify the effectiveness of protective measures.
  - "Detection Processes" and procedures are maintained and tested to ensure timely and adequate awareness of unusual events.
- ***Respond*:** An agency's ability to quickly and appropriately respond to an incident plays a large role in reducing the incident's consequences. As such, the activities within the respond function examine how an agency plans, analyzes, communicates, mitigates, and improves its response capabilities.
  - The "Analysis" category is conducted to ensure adequate response to support recovery activities.
  - The "Communications" category involves communication activities that are coordinated with internal/external stakeholders.
  - "Improvements" describes organizational response activities that can be improved by coordinating lessons learned.
  - "Mitigation" describes the activities performed to prevent the expansion of an event, mitigate its effects, and eradicate the incident.
  - "Response Planning" includes the various procedures that are executed and maintained, to ensure timely response to detected security events.
- ***Recover*:** Activities within the recover function pertain to an agency's ability to return to its baseline after an incident has occurred. Such controls are focused not only on

activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.

- The “Communications” category relates to coordination with internal and external parties during a security event.
- “Improvements” describes the processes related to incorporating lessons learned from handling IT security incidents into improving recovery planning and processes.
- “Recovery Planning” describes processes and procedures that are executed to ensure timely restoration of systems affected by cybersecurity events.

Appendix IV. NCSR Self-Assessment Scoring

Using a maturity scale measurement, each agency evaluates itself on several activities that support each core function. The scale goes from one (*activity is not performed*) to seven (*activity is optimized*). ***The recommended minimum maturity level is set at a score of 5 and higher.***

Score	Rationale	Explanation
7	**Optimized**	Your organization has formally documented policies, standards, and procedures. Implementation is test, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested & Verified**	Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process**	Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
	Risk Formally Accepted	Your organization has chosen not to implement

		based on a risk assessment.
4	**Partially Documented Standards and/or Procedures**	Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy**	Your organization has a formal policy in place.
2	**Informally Performed**	Activities and processes may be substantially performed, and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed**	Activities, processes and technologies are not in place to achieve the referenced objective.

Appendix V. Glossary & Terms

Term	Expansion
BIA	Business Impact Analysis
CIO	Chief Information Officer
CIS	Center for Information Security
CISC	Commonwealth Information Security Council
COV	Commonwealth of Virginia
CSF	Cyber Security Framework (NIST)
CSRM	Commonwealth Security and Risk Management
ECOS	Enterprise Cloud Oversight Service
IDS	Intrusion Detection System
ISO	Information Security Officer
IT	Information Technology
ITRM	Information Technology Resource Management
LAN	Local Area Network
Malware	Malicious code such as viruses, Trojans, ransomware, spyware, and key loggers
MS-ISAC	Multi-State Information Assistance Center
NIST	National Institute of Standards and Technology
PaaS	Platform-as-a-service
Physical Loss	Loss or theft of any COV resource that contains COV data
RCE	Remote Code Execution
RPO	Recovery Point Objectives
SaaS	Software-as-a-Service
SEC530	Information Security Standard 530
Social Engineering	An attack meant to manipulate unsuspecting users to: unknowingly share data with unauthorized individuals or entities, use malicious links, download unauthorized software, transfer funds, or compromise personal or organizational security
SQLi	SQL Injection
Unauthorized Access	Access by individuals who are not vetted and approved to obtain and use specific COV systems and data
VPN	Virtual Private Network
XSS	Cross-Site Scripting