VIRGINIA IT AGENCY

2024 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

Contents

Table of Figures

Background

This 2024 Commonwealth of Virginia (COV) Information Security Report is the 15th 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 the 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 and Appropriations. 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 two Level I institutions of higher education. This report does not address the judicial branch, the legislative branch, various authorities, or 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. In addition, Commonwealth security standards serve only as guidance to local government, and some systems are exempt as described in Section 1.6 of SEC530.

This report uses 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 continued to play a vital role in protecting state IT systems by aligning cybersecurity strategies with national standards and fostering cross-agency collaboration. Commonwealth Security and Risk Management (CSRM), under the direction of the Chief Information Security Officer and the Chief Information Officer (CIO), oversees this comprehensive program. It is designed to monitor compliance, implement security policies, and enhance training initiatives.

In 2024, the Commonwealth participated once again 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 reported strong performance, exceeding the national average. The overall score rose from 5.47 in 2023 to 5.65 in 2024 on a seven-point scale. Agencies continued to show strength in the identify, protect, and detect functions, while opportunities remained in the respond and recover areas. Virginia maintained its standing above peer states, with agencies in sectors such as IT and financial services leading in performance.

Risk management remained a top priority. The IT Risk Management Committee guided the prioritization of risk mitigation efforts, and in 2024, both IT audit and risk compliance findings declined by 2%. CSRM encourages agencies to remain vigilant by continuously monitoring risk activities and implementing appropriate controls to address security gaps.

The Commonwealth's shared services model continued to deliver key security resources for agencies, including centralized IT security auditing, information security officer (ISO) support, and web application vulnerability scanning. In 2024, over 1,600 public-facing websites were scanned monthly to identify vulnerabilities and reduce exposure to threats.

CSRM also promoted knowledge sharing and professional development through its leadership of the Commonwealth Security Information Council, the Information Security Officers Advisory Group, and monthly IT Risk Management Committee meetings. These forums not only foster collaboration but also provide opportunities for security professionals to earn continuing professional education credits and support the continued advancement of cybersecurity capabilities across the Commonwealth.

In conclusion, the Commonwealth's Information Security Program achieved measurable progress in 2024. While areas such as detect and respond still require focused attention, improvements in training, risk oversight, and collaborative engagement continued to elevate the Commonwealth's cybersecurity posture. Ongoing participation in the NCSR and other assessment tools will ensure that agencies have the insights needed to benchmark progress, address gaps and strengthen resilience in the years ahead.

Commonwealth Threat Management

In 2024, VITA continued to enhance the Commonwealth's cybersecurity threat management program by introducing new monitoring tools and refining existing ones.

First, the web vulnerability scanning platform has evolved to support a more aggressive scanning schedule for customer agencies. Monthly scans are now conducted across all agencies, significantly reducing the time between vulnerability identification and remediation. This improvement has strengthened the security posture of both internal and internet-facing systems.

Second, CSRM began rolling out a centralized log aggregation and monitoring solution for executive branch agencies. This tool ingests logs in their native formats, analyzes and correlates data for suspicious activity, and alerts agencies when defined thresholds are met. By consolidating logs from multiple sources, the tool provides a comprehensive, risk-based view of the enterprise. Deployment will continue in 2025.

Third, the Vulnerability Management Platform was introduced in 2024, offering agencies a centralized dashboard to track and address vulnerabilities across operating systems, applications, and websites. Scan results are continuously integrated, enabling agencies to assess their risk posture in real time.

While new security tools enhance protection, human error remains the most significant risk. In 2024, the top three security incident categories were user-related:

1. Information disclosure – 195 incidents
2. Physical theft/loss – 191 incidents
3. Social engineering – 64 incidents

These incidents highlight the need for greater user diligence with Commonwealth-issued devices to prevent data exposure and loss. Although encryption has been implemented for mobile devices, social engineering remains a critical threat. To address this, CSRM introduced continuous phishing simulations, testing COV users at least once a month to strengthen their recognition and response skills.

Cyberattacks against the Commonwealth continued to rise in 2024, with 591 million attempts detected – an average of 18.74 attacks per second – up from 106 million in 2023. This increase is attributed to geopolitical tensions, targeting public entities, and improved attack detection capabilities. Most attempts were successfully blocked by Commonwealth monitoring systems and security tools.

Commonwealth Information Security Governance Program

CSRM annually measures each agency's information security program against the Commonwealth's IT security policies, standards and guidelines. Letter grades were used to summarize the strength of both IT audit and risk management efforts.

To equip security professionals, VITA delivered education and outreach initiatives. Throughout the year, CSRM hosted training sessions, shared enterprise updates and facilitated networking opportunities for the Commonwealth's security community. Agency staff also participated in councils and committees, providing direct feedback on a broad range of security topics.

Third-party risk management remained a core component of the COV risk management program. As reliance on external providers grew, VITA routinely evaluated vendors to ensure they operated within the Commonwealth's risk tolerance. CSRM collaborated with supply chain management and procurement teams, while the COV Ramp group focused on vendors delivering Software as a Service (SaaS) and Platform as a Service (PaaS) solutions. COV Ramp's primary mission is to evaluate the information security programs of potential SaaS and PaaS suppliers to gauge the risk of doing business with them. Contract terms and oversight components are addressed after the initial risk assessment to ensure proper alignment with Commonwealth security standards.

CSRM provided three centralized security services to customer agencies: IT Audit, Information Security Officer (ISO), and Web Application Scanning. The IT Audit and ISO services were subscription-based and helped agencies meet specific security requirements. Web Application Scanning was offered at no discrete cost to the agencies. These services are available as a result of previous investments made by the General Assembly to fund them.

Commonwealth IT Audit and Risk Management Program

IT audit and risk compliance grades shift 4% in 2024. The percentage of above-average IT audit grades declined from 50% in 2023 to 46% in 2024, while above average IT risk compliance grades rose from

58% to 62% over the same period. CSRM distributed quarterly reports to agency ISOs to support ongoing compliance monitoring.

CSRM's risk management team also tracked the progress and remediation of IT audit and risk findings. In 2024, the average age of all open IT audit and risk findings was 1,102 and 1,253 days, respectively. Compared to 2023, the average age of open IT audit findings increased by 154 days, while the average age of open risk findings decreased by 60 days. Most findings resulted from gaps with access control requirements, system integrity (*e.g.*, lacking current security patches), and inadequate third-party hosting agreements. CSRM notified 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 based on the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF). It enables CSRM to evaluate how agencies assess their cybersecurity maturity and benchmark results against other Commonwealth agencies and nationwide participants.

According to the most recent results, Commonwealth agencies achieved an average score of 5.64 (on a 1 to 7 scale) in 2024, an improvement over the previous year and slightly higher than the national average. This score also exceeded the minimum recommended maturity level of 5, which reflects that agencies have formally documented cybersecurity policies, standards and procedures and are actively working to implement them. A total of 35 Commonwealth agencies completed the NCSR assessment in 2024.

Additional information about the NCSR is available at https://www.cissecurity.org/ms-isac/services/ncsr.

Conclusions & Recommendations

Centralized Security Awareness Training Platform

User awareness and training is a key defensive measure to help prevent security incidents.

In 2024, CSRM continued to monitor and support agency-led security awareness training (SAT) efforts by reviewing available training options and providing ISOs with a crosswalk of approved modules. This resource was designed to help agencies build or update their SAT programs in alignment with the Commonwealth's Information Security Standard.

Information Disclosure

Information disclosure incidents accounted for the majority of cybersecurity incidents in 2024. These occur when sensitive information is shared with someone who does not have a need to know, often due to misdirected emails or letters or incorrect database updates. Typically caused by human error, these incidents can be mitigated by reinforcing business processes and enhancing security awareness training. If data is exposed, a security incident should be promptly reported following the appropriate procedures. Examples of information disclosure incident experienced in 2024 are Personal Identifiable Information (PII) being mailed, faxed, or emailed to the wrong address, credentials exposed from

phishing emails, PII being sent unencrypted via email, and citizen users inadvertently accessing agency data records of another user.

Theft or Loss of Electronic Devices

The second most frequent type of cybersecurity incident in 2024 involved the loss or theft of physical electronic devices. Users were reminded to follow Commonwealth policies regarding device handling and to report missing equipment promptly through designated procedures.

Cybersecurity Attacks & Investigations

In 2024, VITA detected over 591 million attempted cyberattacks – averaging approximately 18.74 attempts per second. CSRM conducted or supported more than 1,000 security investigations across the Commonwealth. Agencies were advised to implement appropriate security controls to limit exposure and reduce potential impact until official remediation patches could be applied. CSRM's layered defense-in-depth strategy provided compensating safeguards at multiple levels to help mitigate threats, particularly when remediation was delayed by technical or logistical constraints.

IT Compliance Grades

Overall IT audit compliance grades declined by 4%, while IT risk compliance grades improved by 4%. To help agencies stay on track, CSRM set interim deadlines for agencies throughout the year to monitor key deliverables and support continuous improvement.

Nationwide Agency Self-Evaluation

Commonwealth agencies participating in the 2024 NCSR generally rated themselves at or above the target score of 5, indicating a baseline level of cybersecurity maturity consistent with national standards.

Commonwealth Threat Management Reporting

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, as outlined in security standard SEC530. VITA's Computer Security Incident Response Team (CSIRT) then classifies each report by incident type.

Throughout 2024, the Commonwealth further strengthened its cybersecurity and threat management capabilities. Attempted cyberattacks against state networks climbed 462.86%, topping 591 million attack attempts, while automated defenses blocked more than 114,000 pieces of malware. While the overall risk posture remained relatively steady, there was a sharp increase in information disclosure incidents and the loss or theft of devices such as laptops. These issues highlight the need for additional security awareness training to address user-related vulnerabilities and reduce preventable risks.

Virginia Cybersecurity Planning Committee (VCPC) & Cybersecurity Grant

Virginia continued its participation in the State and Local Cybersecurity Grant Program (SLCGP) in 2024 through analysis of findings from approximately 170 cybersecurity capability assessments conducted with local governments, school districts, and other local public bodies. Recommendations based on this analysis resulted in the approval of vulnerability, secure remote network access, data inventory, asset inventory, communications disaster recovery, endpoint detection and response, and firewall services as the next area of focus for SLCGP projects with local government entities. Grant applications for projects in these areas were opened in late 2024 and approximately 140 local government entities submitted applications by the due date.

While Virginia's approach to the SLCGP is different from many grant programs, it remains dedicated to managing and reducing systemic cyber risk through the objectives outlined in SLCGP Notices of Funding Opportunity. Additional information about Virginia's participation in the SLCGP is available in the annual report specifically concerning that program.

Centralized Incident Reporting: Virginia Fusion Center

To improve statewide threat intelligence, Virginia Code § 2.2-5514 was amended in 2022 to require all public bodies to file incident reports with the Virginia Fusion Center. Before that change, limited reporting from local governments and high education institutions had left notable blind spots in the Commonwealth's risk picture and hampered the design of effective countermeasures. Since the law's enactment, CSRM has begun receiving critical incident data from those previously underrepresented sectors, expanding visibility into emerging threats facing Virginia public bodies.

Cybersecurity Incidents

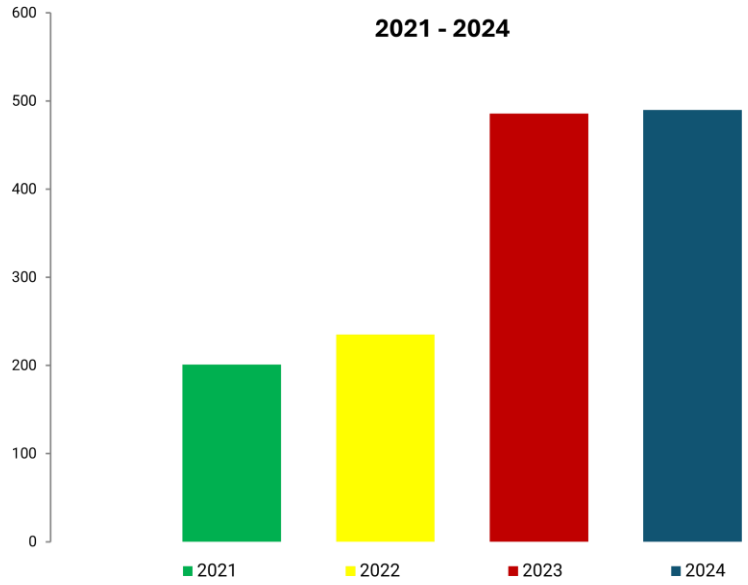
Cybersecurity incidents remained prevalent in 2024, with a total of 450cases reported across the Commonwealth. The top three incident types were information disclosure, physical device loss, and social engineering.

Information disclosure was the most common, accounting for 195 incidents. These occur when sensitive information is shared with unauthorized individuals, often due to misdirected emails or letters, or data entry errors linking records to the wrong file. Most result from human error and can be mitigated through enhanced security awareness training.

Lost or stolen Commonwealth devices ranked second, with 191 incidents. While this marks a slight improvement from 2023, it remains a significant risk, reinforcing the need for encryption on all mobile devices.

Social engineering ranked third, with 64 incidents. The increase is largely due to improved reporting, aided by the ongoing use of the Phishing Alert Button (PAB), which streamlines reporting and email removal.

Figure 1. Total Cybersecurity Incidents by Year



As technology use increases, so does the risk of information disclosure. Users rely on laptops, tablets and smartphones for tasks like checking email, updating records and drafting communications. However, autofill and auto-correct can mistakenly select the wrong recipient, leading to unintended disclosures. To mitigate this risk, users must carefully review their work, as even correctly typed information can be altered by these tools. Additionally, all sensitive electronic communications should be encrypted. Ultimately, only diligent human oversight can prevent these incidents.

Physical loss or theft of COV devices remained the second most common incident in 2024, often resulting from users' lack of awareness and failure to maintain custody of their devices. As with information disclosure incidents, prevention relies on human vigilance and security awareness training.

Social engineering incidents decreased in 2024, dropping to the third most common type and accounting for 13.06% of all reported incidents. This decline was supported by CSRM's enterprise-wide security awareness training, which equips users with the knowledge to recognize and respond to threats. Key topics include safe browsing, identifying suspicious emails, using encryption, responding to threats, and reporting incidents. Additionally, over nine million emails were blocked to protect COV users from these types of attacks. With legislative support, CSRM continues to enhance this program. In 2024, CSRM completed the rollout of an enterprise-wide training platform, increasing the frequency of simulated phishing campaigns to once every 30 days. To continue the improvement in this area, security awareness training must remain a priority for all COV users.

In 2024, more than 114,000 pieces of malware were blocked. Despite these preemptive measures, malware attacks accounted for 90% of cybersecurity incidents, remaining a pervasive threat. The rise in attacks followed cyclical patterns of online activity, such as holiday shopping and tax season. However, Commonwealth security solutions effectively blocked over 99.98% of malware threats.

Figure 2. Cyber Incidents by Category

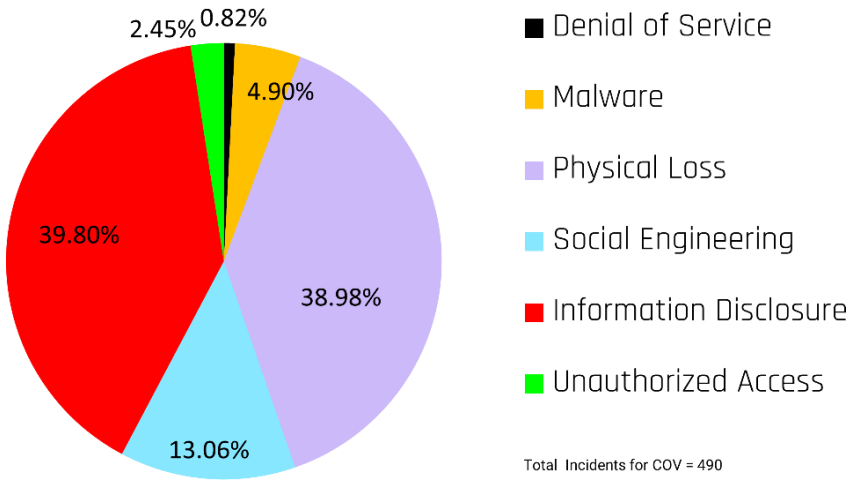


Figure 3. P1 Incident Trends 2021-2025

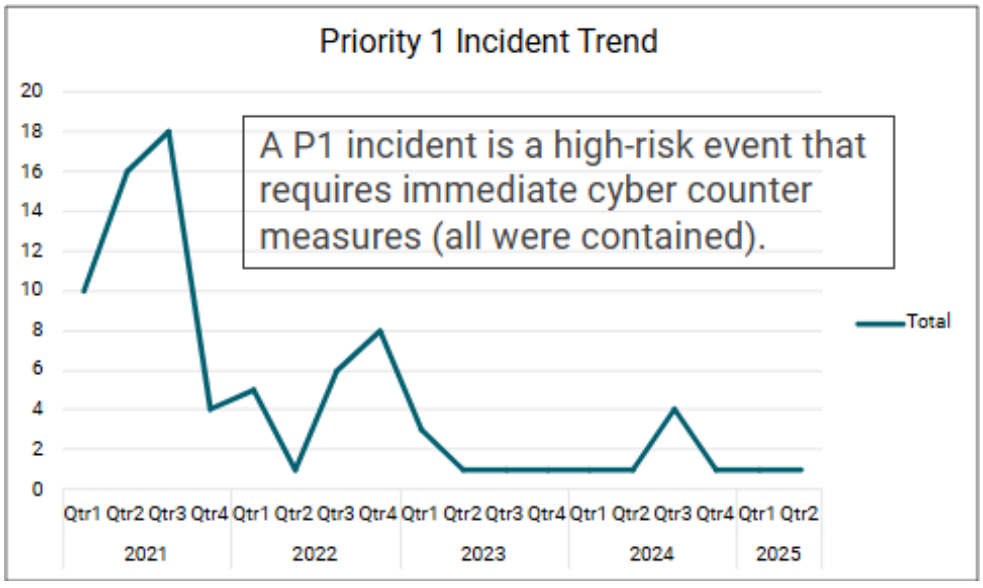
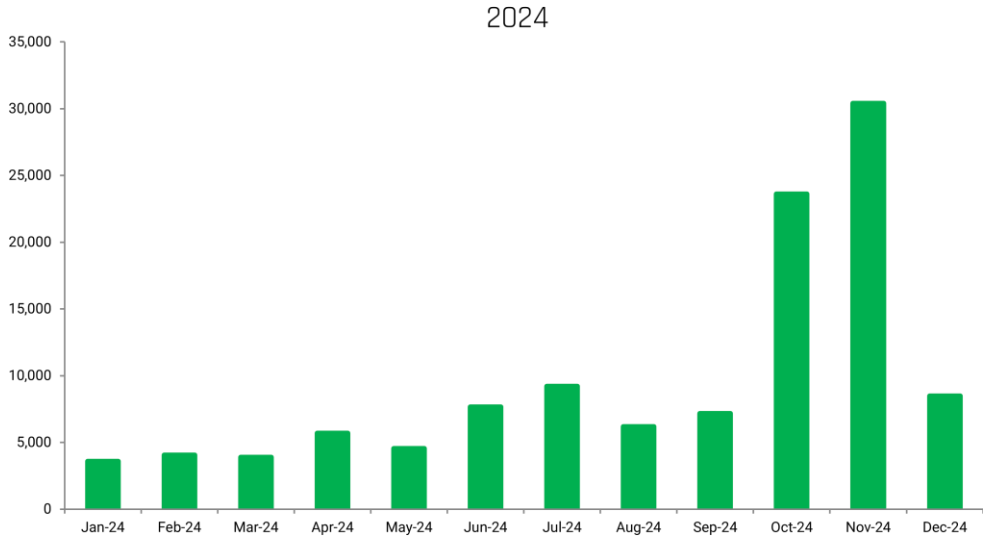


Figure 4. Malware Blocked



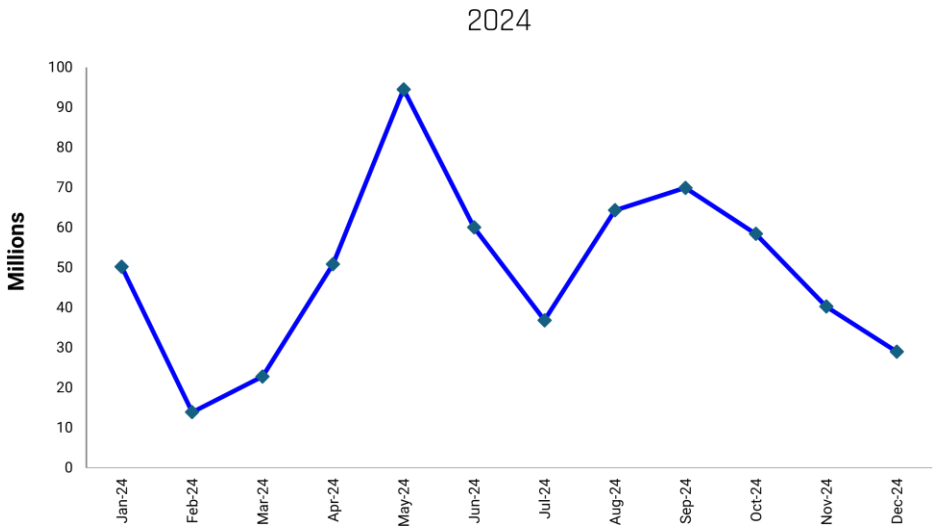
Although the total number of cybersecurity incidents in 2023 and 2024 have increased (see Figure 1), the number serious incidents (classified as P1 incidents) has substantially gone down from a high of 18 per quarter to an average of only 1 per quarter. The ongoing investments in strengthening Commonwealth cybersecurity tools, policies, and practices are showing results. We are detecting more potential problems (shown as more total incidents) and rapidly clearing and remediating them before they caused greater impact to the Commonwealth.

In 2024, more than 114,000 pieces of malware were blocked. Despite these preemptive measures, malware attacks accounted for 90% of cybersecurity incidents, remaining a pervasive threat. The rise in attacks followed cyclical patterns of online activity, such as holiday shopping and tax season. However, Commonwealth security solutions effectively blocked over 99.98% of malware threats.

Cybersecurity Attacks

In 2024, Commonwealth systems detected 591 million attack attempts—an average of 18.74 per second. Spikes in activity often indicate emerging attack methods or improved detection capabilities. When an alert is triggered, traffic is analyzed to distinguish between malicious and authorized activity. Systems are then adjusted to block threats while fine-tuning alerts for known authorized traffic to reduce false positives. The resulting decline in attack attempts after a spike reflects this continuous system optimization.

Figure 5. Attack Attempts on COV Networks



In 2024, most attacks on the Commonwealth originated in the United States. CSRM closely monitors attack origins, integrating threat intelligence from multiple sources into security monitoring systems to protect Commonwealth data. This intelligence is shared with partners, enabling proactive blocking of threats before systems are compromised. Over the past year, the top sources of attacks were the United States, followed by the Netherlands, France, Singapore, and Malaysia. However, proactive geographical traffic controls block interactions with high-risk regions, such as China, Russia, and Ukraine, which is why these countries are not represented in the data.

Figure 6. Top Five Attack Origins

Exploits and Vulnerabilities

CSRM is developing a centralized system that enables agencies to manage operating system application and web application vulnerabilities using a single platform. This system consolidates scan results from multiple sources, providing real-time visibility into each agency's risk posture. Vulnerabilities are assigned to the appropriate teams for remediation, and future enhancements will include automated ticketing to streamline the process.

The global vulnerability dashboard has helped CSRM identify gaps and remediation challenges, such as end-of-life software, unavailable patches, or uncertainty over patching responsibilities. Addressing these issues will strengthen the Commonwealth's overall cybersecurity posture moving forward.

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.

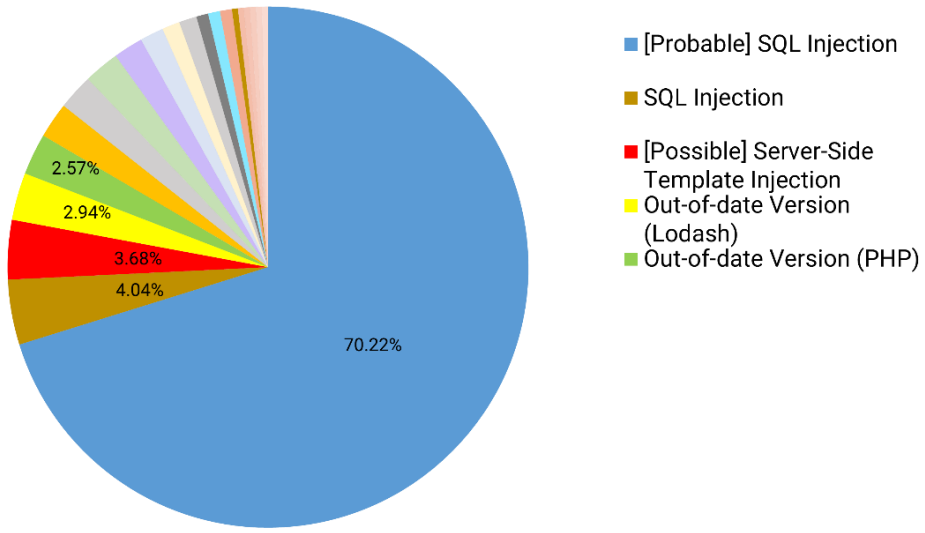
When an SQLi attack occurs, the vendor or developer must remediate the vulnerability, and database administrators must validate the database's data. In some cases, data breach notifications may also be required.

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 7. Top 5 Critical Web Vulnerabilities



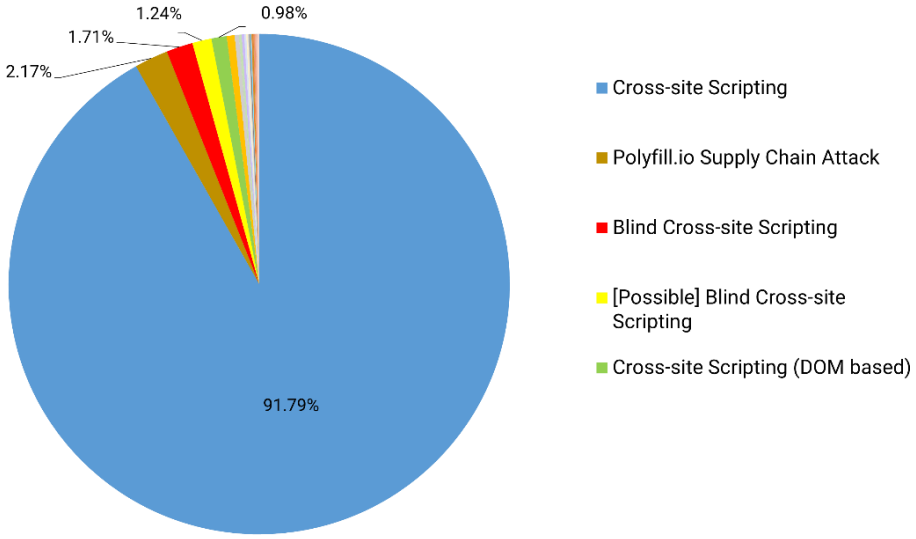
Top High Vulnerabilities

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 8. Top 5 High Web Vulnerabilities



Security Investigations

The information received from Commonwealth partners, including other states, 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 usually 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. The total number of investigations decreased in 2024 by 40%. This is due to less intelligence being received from our third-party partners. Of the investigations completed in 2024, 48.25% fall into the Other category which includes inappropriate use, information disclosed but not used by attackers, lost and found devices, mis-mailings, and threat intelligence information that was received.

Figure 9. Security Investigations by Entity

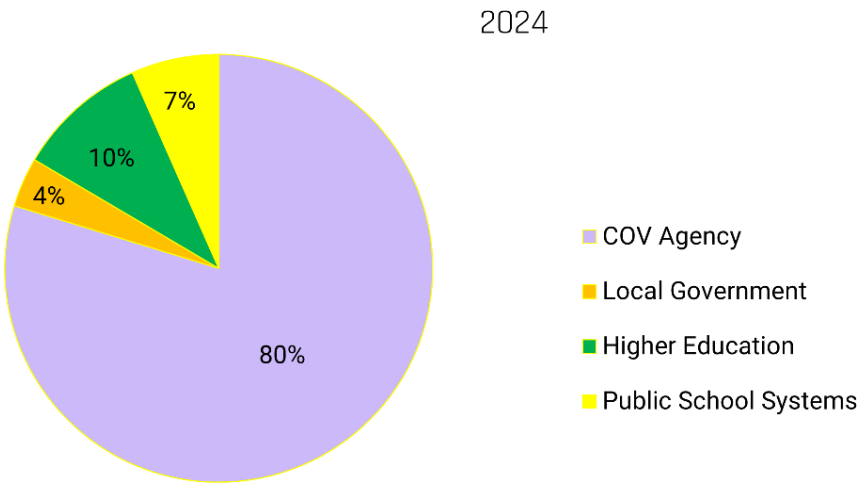
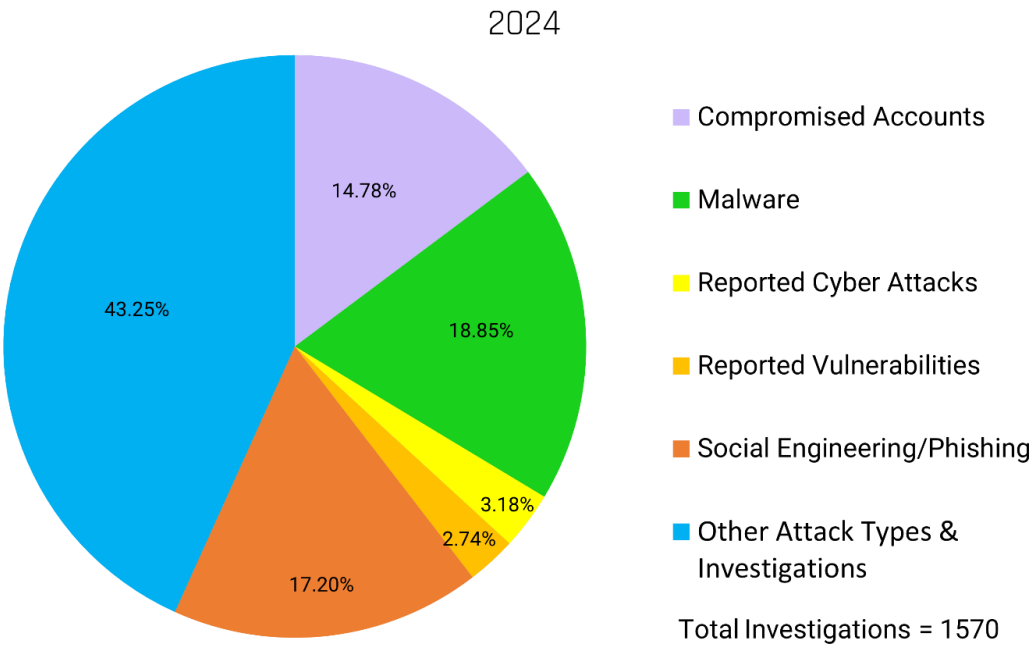


Figure 10. Security Reference Plan by Category



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

The **Information Security Governance Program** ensures that Commonwealth agencies maintain strong compliance with established information security policies, standards, and risk management practices. As required by § 2.2-2009(B)(1) of the Code of Virginia, the CIO must report on the results of security audits, the extent to which agencies have adopted required security policies and standards, and agencies that have not implemented adequate controls to mitigate unauthorized access, intrusions, or other threats.

To fulfill this mandate, CSRM operates the Information Security Governance Program to monitor each agency's overall compliance with IT audit and information security risk program standards. This includes tracking the completion of required audits, reviewing risk management practices, and ensuring agencies are aligned with statewide cybersecurity expectations. The program provides transparency, supports continuous improvement, and enables strategic oversight of the Commonwealth's information security posture.

Security Awareness Training and Phishing Campaigns

In 2024, CSRM continued to offer enterprise-wide security awareness training.
User training is essential to the protection of publicly-owned assets. VITA's security awareness training service is a centralized solution available to all Commonwealth agencies, not just executive branch agencies under VITA purview. This remains a critical focus area because 86% of categorized incidents were tied to user error or mishandling of devices or data, not social engineering. These types of incidents highlight the ongoing need for regular, targeted awareness training to reduce risk and improve cybersecurity posture across the Commonwealth.

CSRM has developed a free simulated phishing service to supplement security awareness training. Using the latest threat intelligence, the CSRM threat management team designs campaigns to help Commonwealth users recognize common phishing attacks. These campaigns reinforce key concepts from training and serve primarily to assess the effectiveness of users' security awareness. Campaigns were migrated from a quarterly to a monthly basis in 2024 to allow COV users to stay up to date with the new techniques attackers are using.

ISO Orientation and Certification

CSRM offered both introductory and recertification training courses for Commonwealth information security officers (ISOs). The sessions outlined the state's information security program, core processes, available services and key CSRM contacts. In 2024, CSRM delivered virtual classes to 122 participants. Dates and registration information was regularly announced on the VITA website, and

CSRM urged newly appointed ISOs to enroll as soon as they assumed their duties. Recertification is required every two years to ensure ISOs remain current with program expectations and evolving cybersecurity practices.

Information Security Officer Advisory Group (ISOAG)

The Information Security Officers Advisory Group (ISOAG) welcomes security professionals from state and local government. Its mission is to strengthen the Commonwealth's security posture through knowledge-sharing. Throughout 2024, CSRM hosted monthly ISOAG meetings that featured presenters from government and industry at no cost to attendees. Participation earned continuing-professional-education (CPE) credits, supported discussion of best practices, and offered feedback channels for proposed policy updates. Presentation materials were posted on the VITA website, and average monthly attendance reached 200.

Commonwealth Security Information Council (CISC)

A select group of agency information security officers, supported by CSRM, constitutes the Commonwealth Information Security Council. The council advised on strategic direction for security and privacy initiatives in the Commonwealth. In 2024, it focused on deepening members' understanding of agency business processes, building consensus for enterprise-wide security projects, highlighting opportunities for improvement and aligning agency operations with VITA procedures. CSRM continued to consult the council for practical input on future initiatives.

IT Risk Management Committee

Risk specialists from CSRM and agency ISOs make up the IT Risk Management Committee. The committee met monthly to discuss significant risks, set mitigation priorities and evaluate whether existing controls held risk within approved thresholds. It documented and escalated risk alerts that could affect the enterprise or customer agencies. Those efforts helped VITA, agencies, and service providers make notable progress in reducing potential threats and impacts.

Third-Party Risk Management

CSRM maintained formal methods for monitoring and managing risks introduced by external service providers. By quantifying third-party risk, the Commonwealth ensured it stayed within established thresholds. CSRM also played a key role in the multi-sourcing integration model, identifying cybersecurity issues and tracking them through resolution – allowing VITA and its vendors to address threats before they could affect Commonwealth data and systems.

As demand for cloud services continued to rise, CSRM ran a security review process for third-party systems. The COV Ramp service managed contract terms and oversight for Software as a Service (SaaS) and Platform as a Service) vendors. CSRM preformed pre-contract assessments to verify that required controls were in place before deployment.

Table 1. 2017-2024 COV Ramp Assessments

COV Ramp	2017	2018	2019	2020	2021	2022	2023	2024

# of Assessments by Date Submitted	75	89	82	70	148	100	136	99
# of Assessments by Date Completed	24	68	76	53	101	86	123	74
Avg Entering Active Oversight	17	48	53	37	71	60	86	82
Avg Cumulative Total Oversight	17	65	118	155	226	286	372	454

Centralized Shared Security Services

To strengthen agency IT security programs, CSRM provided a suite of centralized shared services. These services included IT security auditing, ISO support, and web application vulnerability scanning programs. The audit and ISO support services were optional and available to agencies based on their specific needs, while web application scanning was a mandatory service used to detect vulnerabilities in agency websites and recommend mitigation actions. Together, these services helped improve overall security posture and compliance across the Commonwealth.

Centralized IT Audit Service

Historically, many agencies lacked the internal resources or funding to conduct required IT security audits. CSRM's centralized audit service addressed this gap by helping agencies document audit plans, conduct the audits and develop corrective action plans in response to findings. In 2024, 32 agencies used the shared centralized audit service to fulfill their IT security audit requirements.

Shared ISO Service

In 2024, 28 customer agencies subscribed to CSRM's Shared ISO service. The program supported smaller agencies with limited security resources in maintaining essential IT risk management documentation, including business impact analyses (BIAs), risk assessment plans and individual IT system risk assessments.

Web Application Vulnerability Scanning

CSRM conducted automated scans of more than 1,600 public-facing Commonwealth websites each month in 2024 to detect potential security vulnerabilities. These scans enabled agencies to identify and remediate issues before they could be exploited.

IT Audit Compliance & IT Risk Compliance

CSRM oversaw agency information security programs to verify that minimum IT audit and risk management requirements were met in accordance with Commonwealth policies. Under §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.

CSRM used predefined metrics to assess agency performance for the calendar year. Scores were calculated on a 10-point scale and converted into letter grades (A through F) to offer a clear and familiar indication of compliance status. These grades highlighted both strengths and areas for improvement in each agency's security program.

The Commonwealth's IT audit compliance program included reviewing agency-submitted IT audit plans, conducting audits and submitting corrective action updates. Final scores reflected the agency's progress in submitting plans, providing quarterly updates on audit findings and completing required audits.

Similarly, the Commonwealth IT risk management program reviewed the completeness and quality of agency submissions, including data sets, business impact analyses (BIAs), risk assessment plans, risk assessment findings updates, ISO certification reports and intrusion detection reports. These components determined each agency's overall risk compliance score, which reflected the maturity of its risk management efforts.

2024 IT Audit and Risk Compliance and Grades

In 2024, 46% of IT Audit compliance grades were above average, an A or B. Overall audit compliance grades decreased by 4% in 2024. CSRM recommends that agencies continue to complete required audits, audit plans, and provide quarterly findings updates.

In 2024, 62% of IT risk compliance grades were above average.

Overall, IT risk compliance increased 4% in 2024. CSRM recommends that agencies continue to satisfy risk management requirements.

Figure 11. 2020-2024 Audit Compliance Grades

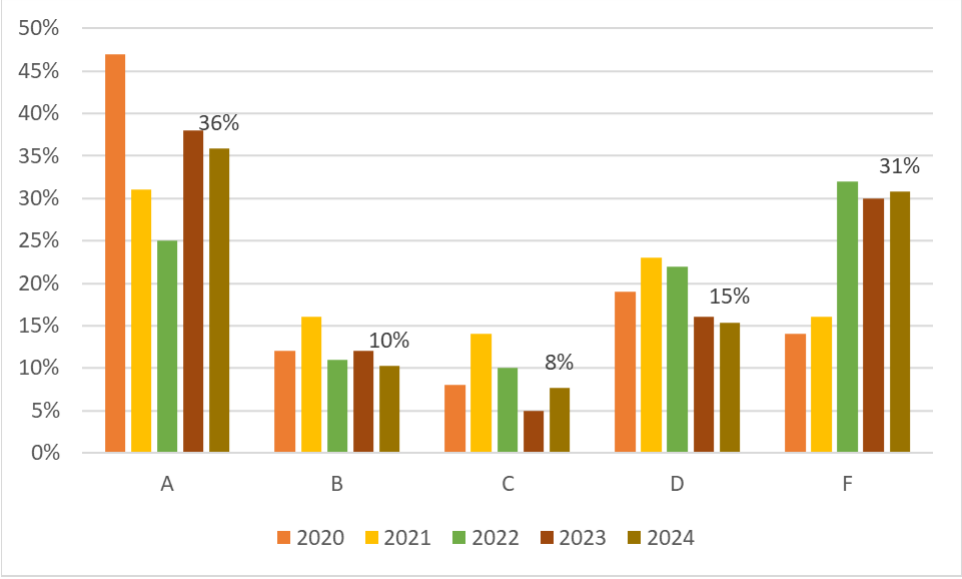


Figure 12. 2024 IT Audit & Risk Compliance Analysis

2024 IT Audit & Risk Compliance Analysis				
Program	**Metric**	**Full Compliance Rate**	**1 Year Change**	**Notes**
Audit	Audit Plan	78%	4% decrease	
	3 Year Audit Obligation	24%	5% Decrease	45% partial compliance
	Current Year Percentage of Quarterly Findings Updates Received: Audit	58%	1% increase	26% partial compliance
Risk	Risk Assessment Plan	82%	7% increase	
	3 Year IT Risk Assessment Obligation	28%	1% increase	33% partial compliance
	Business Impact Analysis (BIA) Status	59%	3% decrease	13% partial compliance
	Current Year Percentage of Quarterly Findings Updates Received: IT risk assessments	67%	1% increase	27% partial compliance
	Quarterly Intrusion Detection Systems (IDS) reports are received	88%	6% decrease	
	Applications Certified	81%	9% decrease	10% partial compliance

	ISO Certification Status	76%	10% decrease	
	ISO Reports to Agency Head	86%	2% increase	

IT Audit and IT Risk Findings

CSRM'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 2024, CSRM reports the average age for all open IT audit and risk findings is 1,102 and 1,253 days respectively. To reduce risk, CSRM requires agencies to implement mitigating controls for any findings or exceptions that are not being remediated in a timely manner. Exceptions should be formally filed when timely remediation is not possible. CSRM also recommends regular reviews of findings to ensure mitigating controls remain effective and risk is being managed appropriately.

Access Control Remains the Most Common Audit and Risk Finding. Although there has been a notable decrease from last year's 33%, access control remains the largest control family, accounting for 17% of all audit and risk findings across the Commonwealth.

Figure 13. 2024 Findings by Secretariat

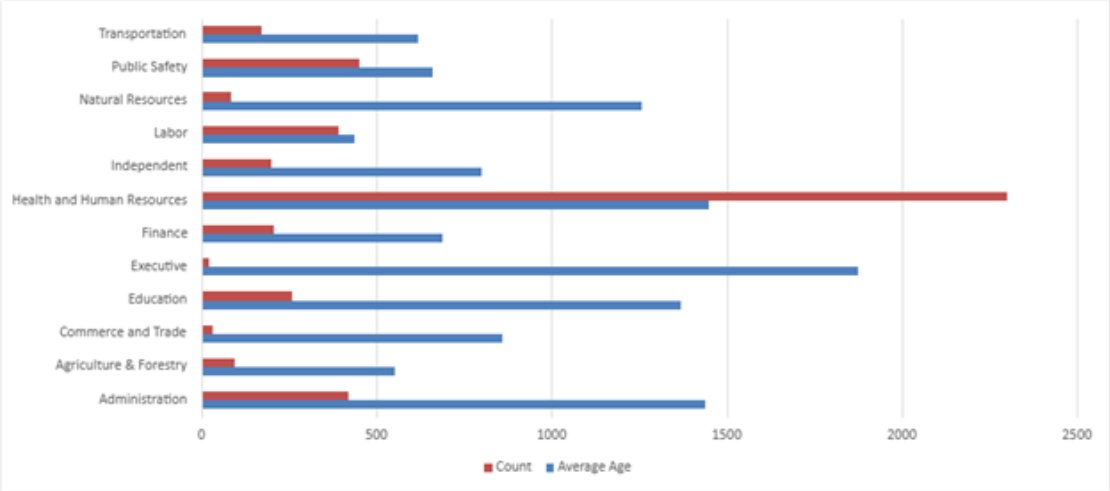
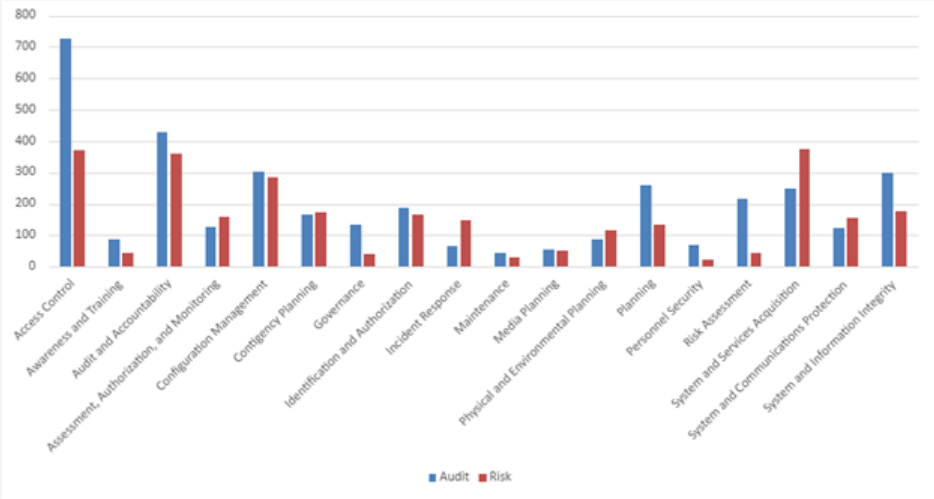


Figure 14. Audit and Risk Findings by Security Control Family



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 United States Congress.

The NCSR provides significant insight into IT security practice at each agency by identifying gaps in performance areas that allow VITA 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 its performance on a maturity scale for five core cybersecurity functions: *identify, protect, detect, respond and recover*. The maturity scale ranges 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.

2024 Assessment Survey

In 2024, 45 states participated in the NCSR assessment, including Virginia, with participation by 35 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. CSRM recommends Commonwealth agencies continue to participate in the assessment to identify opportunities to improve information security programs and security services.

Peer Assessment

In 2024, the average maturity score for CSF functions for the Commonwealth is 5.65 (on a 7-point scale), up from 5.47 in 2023.

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 identify, protect, and detect functions with lower maturity in the 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. 2024 Commonwealth (COV) averages compared to other state agencies and states

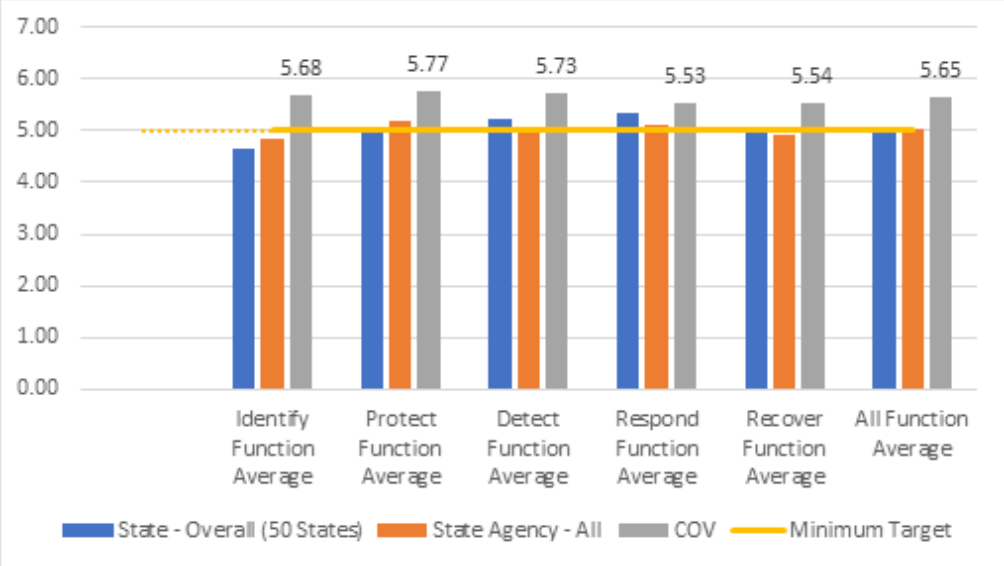


Figure 16. 2024 Commonwealth (COV) Identity function peer assessments by sub sector

Figure 17. 2024 Commonwealth (COV) Protect function peer assessments by sub sector

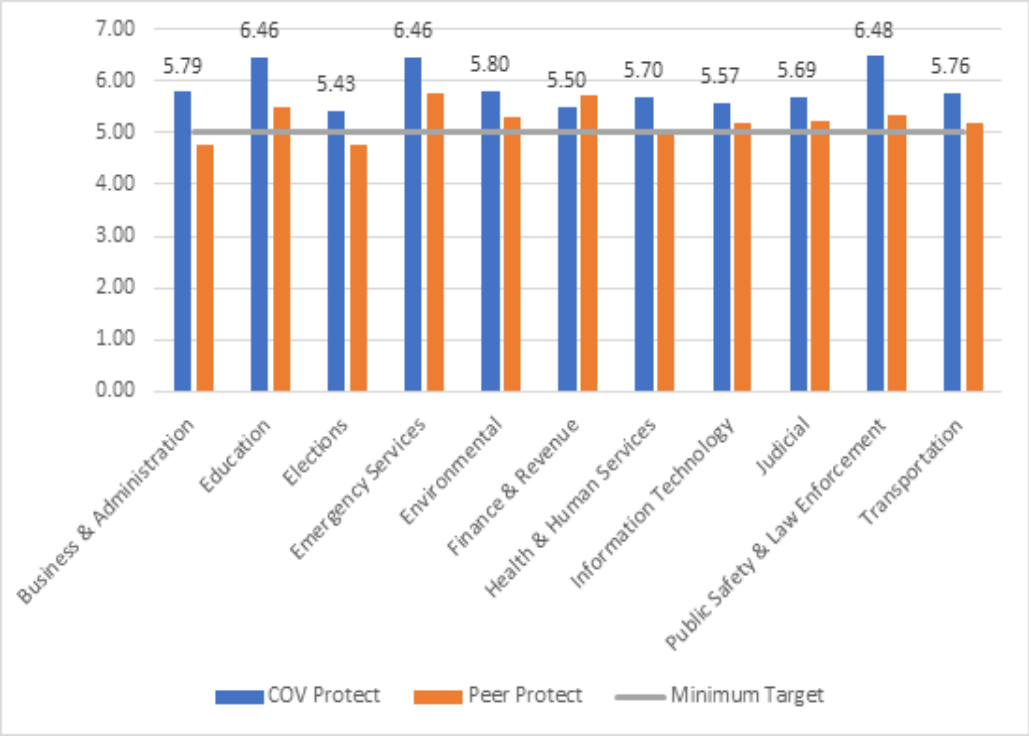


Figure 18. 2024 Commonwealth (COV) Detect function peer assessment by sub sector

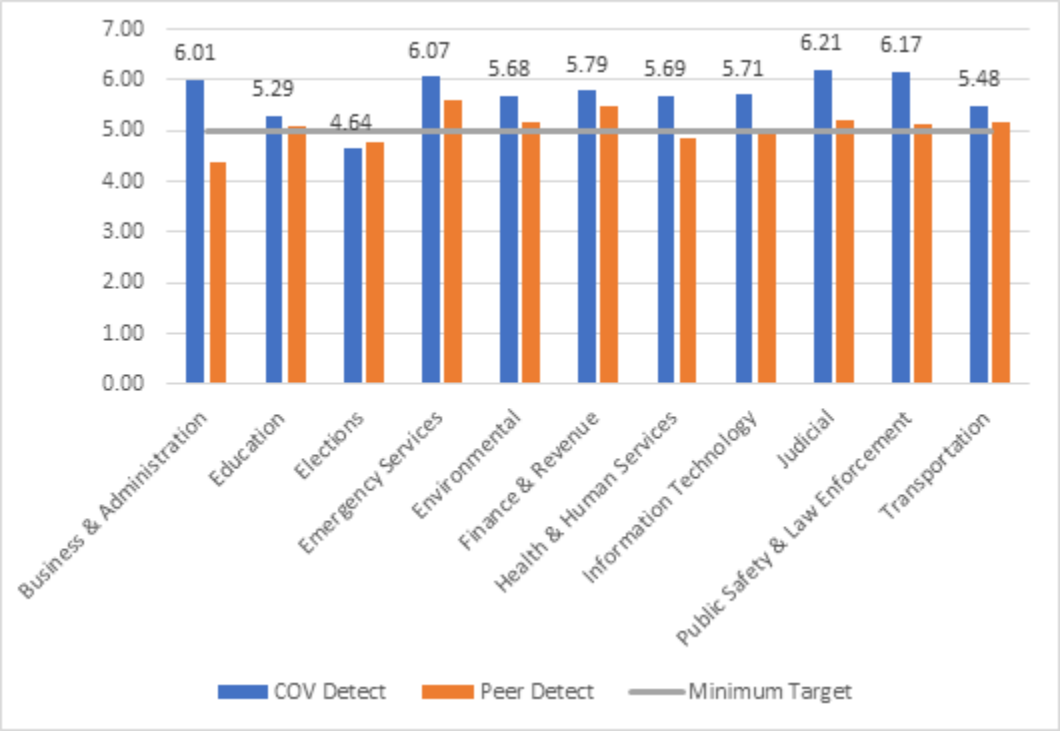


Figure 19. 2024 Commonwealth (COV) Respond function peer assessment by sub sector

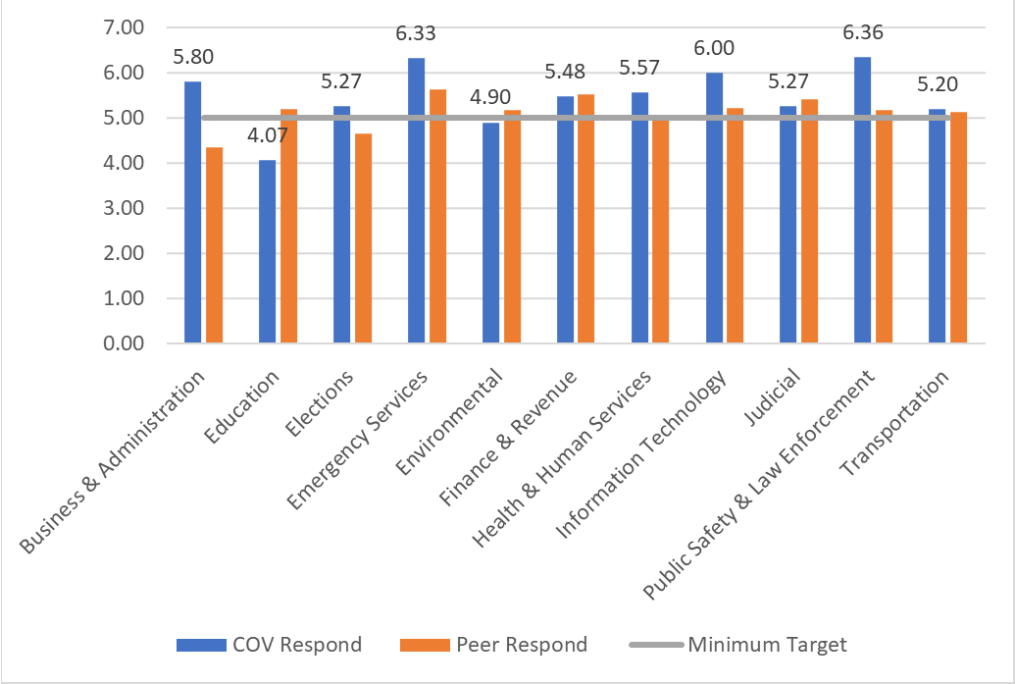
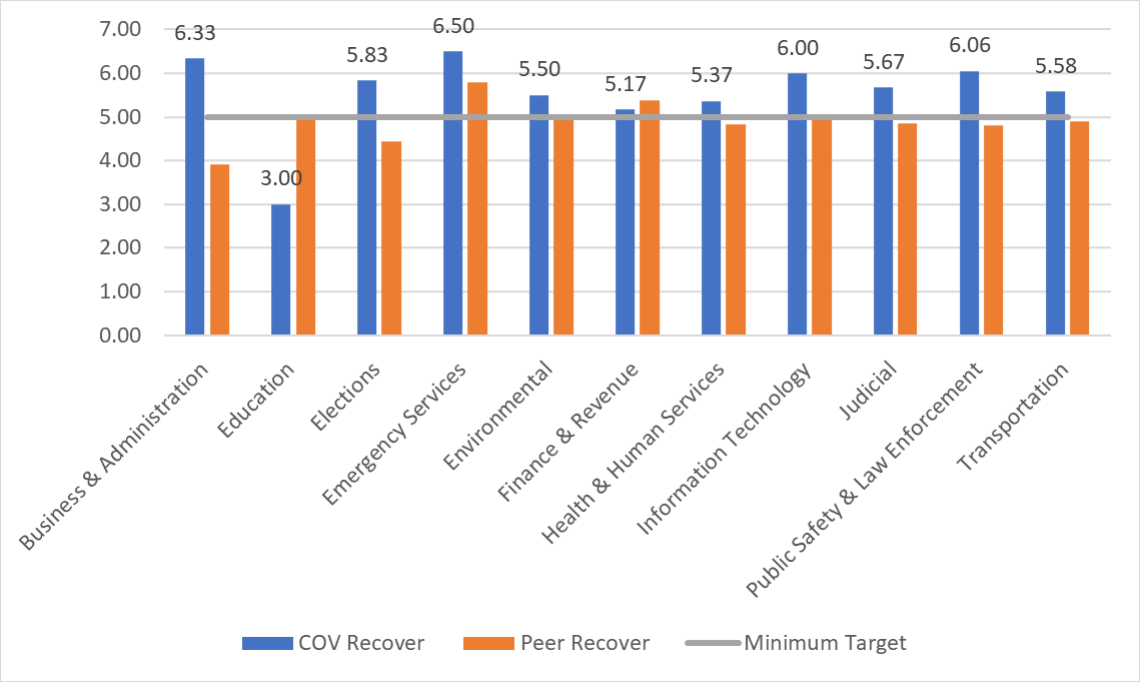


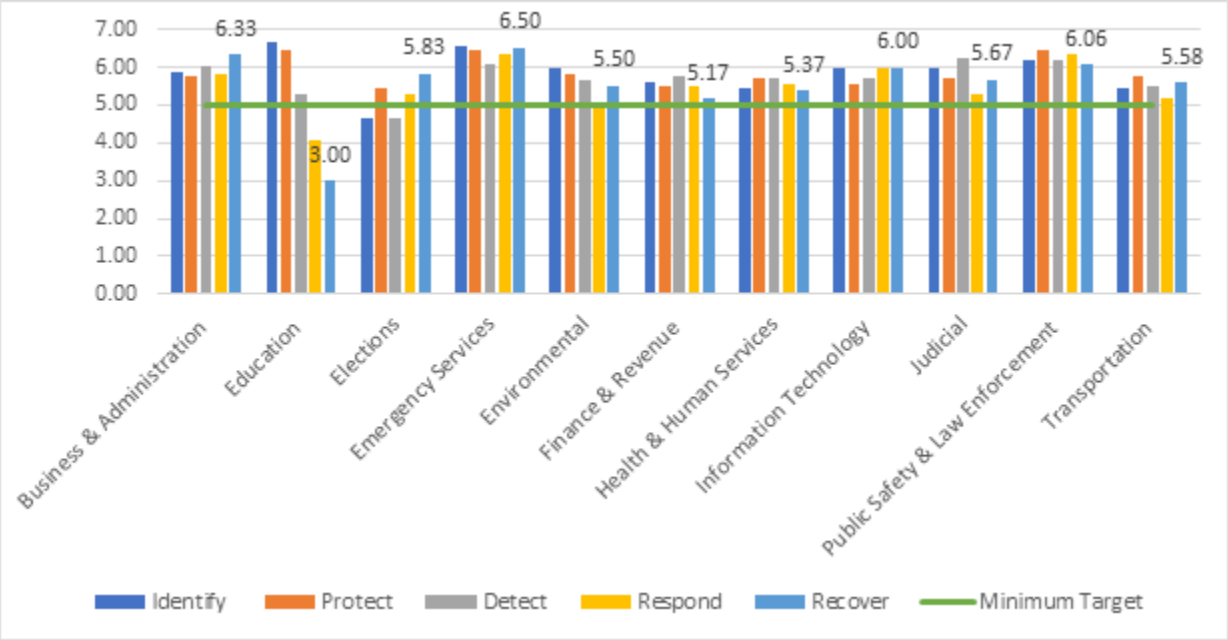
Figure 20. 2024 Commonwealth (COV) Recover function peer assessment by sub sector



Commonwealth Self-Assessment

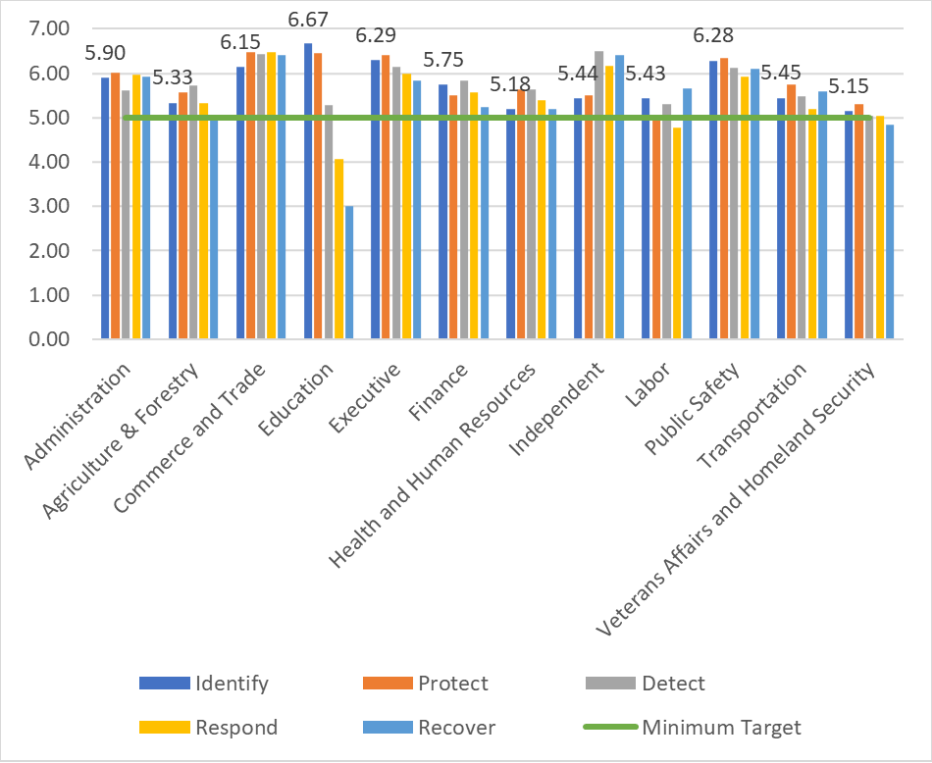
In 2024, the Commonwealth's emergency services, public safety and law enforcement sectors report higher maturity scores in all functions. Commonwealth education and higher education organizations report lower maturity scores. Commonwealth education organizations report higher maturity in the identity and protect functions but significantly lower maturity levels in the respond and recover functions.

Figure 21. 2024 Commonwealth (COV) Functional self-assessment by sub sector



Most Virginia secretariats report at least one functional area meeting the recommended maturity level of 5. Overall, agencies continue to report lower scores in the respond and recovery functions.

Figure 22. 2024 Commonwealth (COV) Functional self-assessment by secretariat



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

Appendix II. 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 III. 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 and 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 IV. 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 Sharing and Analysis 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