2022 Commonwealth of Virginia Information Security Report

Submitted in compliance with the Code of Virginia (§2.2-2009)

Comments on the 2022 Commonwealth of Virginia Information Security Report are welcome.

Electronically send comments and suggestions to:

cio@vita.virginia.gov

Please submit written correspondence to:

Chief Information Officer

Commonwealth Virginia Information Technologies Agency

Boulders VII

7325 Beaufont Springs Drive

Richmond, Va. 23225

Contents

1. Executive Summary 6

1.1. Commonwealth Threat Management 6

1.2. Commonwealth Information Security Governance Program 7

1.3. Commonwealth IT Audit and Risk Management Program 7

1.4. Nationwide Cyber Security Review 8

1.5. Conclusions & Recommendations 8

1.5.1. Centralized Security Awareness Training Platform 8

1.5.2. Theft or Loss of Electronic Devices 8

1.5.3. Cybersecurity Attacks & Investigations 8

1.5.4. IT Compliance Grades 8

1.5.5. Nationwide Agency Self-Evaluation 8

2. Commonwealth Threat Management Report 9

2.1.1. Virginia Cybersecurity Planning Committee (VCPC) & Cybersecurity Grant 9

2.1.2. Centralized Incident Reporting – Virginia Fusion Center 9

2.2. Cybersecurity Incidents 9

Cybersecurity Incidents Increased 15% in 2022. 9

Physical Theft or Loss of Electronic Devices Increased in 2022. 10

More than 73,000 Pieces of Malware Blocked in 2022. 10

Information Disclosure Incidents Decreased in 2022. 10

2.3. Cybersecurity Attacks 12

2.4. Exploits and Vulnerabilities 14

2.5. Commonwealth Web Applications 15

2.6. Security Investigations 17

3. Commonwealth Information Security Program 19

3.1. Information Security Governance Program 19

3.2. Security Awareness Training and Phishing Campaigns 19

3.3. ISO Orientation and Certification 19

3.4. Information Security Officer Advisory Group (ISOAG) 20

3.5. Commonwealth Security Information Council (CISC) 20

3.6. IT Risk Management Committee 20

3.7. Third Party Risk Management 20

3.8. Centralized Shared Security Services 21

3.8.1. IT Audit Service 21
3.8.2. Shared ISO Service 21
3.8.3. Web Application Vulnerability Scanning 21
3.9. IT Audit & IT Risk Compliance 21
3.9.1. 2022 IT Audit and Risk Compliance and Grades 22
3.9.2. IT Audit and IT Risk Findings 24
4. Nation-wide Cybersecurity Review (NCSR) Assessment 27
4.1. NCSR Assessment Background 27
4.2. 2022 Assessment Summary 27
4.3. Peer Assessment 27
4.4. Commonwealth Self-Assessment 29
Appendix I. Information Security Program Metrics 32
Appendix II. NCSR Self-Assessment Standards 33
Appendix III. NCSR Self-Assessment Scoring 35
Appendix IV. Agency Information Security Data Points 36
Appendix V. Glossary & Terms 39

List of Figures

Figure 1. 2022 Cyber Incidents by Category 11
Figure 2. Malware Blocked 11
Figure 3. Historical Cyber Incident Trends 12
Figure 4. Historical Cyber Incident Trends by Category 12
Figure 5. Attack Attempts on COVA Networks 13
Figure 6. Top Five Attack Origins 14
Figure 7. Critical Vulnerabilities Yearly Trend 15
Figure 8. Web Application Exploits by Quarter 16
Figure 9. Top Five High Web Application Vulnerabilities 17
Figure 10. Top Five Medium Web Application Vulnerabilities 17
Figure 11. Security Investigations by Entity 18
Figure 12. Security Investigations by Category 18
Figure 13. 2019 – 2022 Audit Compliance Grades 23
Figure 14. 2019 – 2022 Risk Compliance Grades 23
Figure 15. 2022 Findings by Secretariat 25
Figure 16. 2022 Audit Findings By Security Control Family 25
Figure 17. 2022 Risk Findings By Security Control Family 26
Figure 18. Commonwealth (COV) compared to state Peers and Sub -Sectors 28
Figure 19. Commonwealth (COV) Agencies by Sub-Sector 29
Figure 20. Commonwealth (COV) Agencies by Secretariat 30

List of Tables

Table 1. 2022 IT Audit & Risk Compliance Analysis 24
Table 2. 2022 NCSR Self-Scoring Results 31

1. Executive Summary

This 2022 Commonwealth of Virginia (COV) Information Security Report is the 13th 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, and Level II and Level III higher education institutions, which are either statutorily exempted 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.

1.1. Commonwealth Threat Management

The Commonwealth took significant action in 2022 to improve cybersecurity threat management throughout the state. Using a federal grant program for cybersecurity, the Commonwealth took action to help mature cybersecurity programs throughout the state in 2022. The Commonwealth also ratified legislation to improve threat intelligence analysis and defense planning.

The number of Physical Theft/Lost Security incidents increased from 52 to 103 in 2022. This was the leading category of incidents in 2022. Theft and lost incidents are attributed to the user, who need to be more cognizant of the environment and location of their COV-issued devices. Successful malware incidents increased from 26 in 2021 to 53 in 2022.

CSRM continues to invest in security awareness training. End users face new and evolving security concerns regularly. In an effort to keep pace with threats and common attacks, CSRM uses simulated phishing exercises to supplement annual security awareness training material. Quarterly phishing campaigns help hone recognition and incident response skills.

In 2022, the number of attacks against the Commonwealth continued to increase. 55 million attacks attempts were detected against Commonwealth systems – a rate of 1.75 attacks every second, up from approximately 33 million attacks in 2021. Most attacks are blocked and prevented by Commonwealth monitoring systems and security tools.

Addressing web application vulnerabilities requires agency support. Malicious attackers use a myriad of techniques to infiltrate systems and gain access to information, such as exploits (e.g., viruses, worms) and vulnerabilities (i.e., system flaws). In 2022, CSRM successfully blocked most exploits, despite an uptick in exploit activity. Critical and high vulnerabilities in internet facing web applications were identified and tracked. CSRM recommend agencies continue to apply patches and remediate prioritized vulnerabilities.

1.2. 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 for IT audit and IT risk management programs.

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

Third Party risk management is a key component of the COV Risk Management program. Demand for third party services continues to increase. To review concerns with third party vendors, CSRM Risk Management integrates with supply chain management. The Enterprise Cloud Oversight Service (ECOS) reviews and approves contract terms and provides oversight of third-party vendors offering Software-as-a-Service (SaaS) 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.

1.3. Commonwealth IT Audit and Risk Management Program

IT Audit and Risk compliance grades declined in 2022. While 36% of the IT audit compliance grades were above average, the percentage of failing grades increased to 32%. CSRM attributes this to a decline in the number of IT audits performed in 2022. CSRM anticipates audit program compliance will improve as agencies plan to complete required audits. Many IT risk grades were reduced by a letter grade due to missing risk assessment plans outlining the schedule to complete required risk assessments. Missing or inadequate quarterly updates also had a negative impact on IT Audit and Risk grades in 2022.

CRSM's Risk Management team also monitors the progress and remediation of IT audit and risk findings. In 2022, the average age for all open IT audit and risk findings was 807 and 1,240 days, respectively. 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.

1.4. 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 with 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 2022 was 5.49, which is slightly above the minimum recommended level of 5. In 2022, 39 Commonwealth agencies participated in the NCSR assessment.

1.5. Conclusions & Recommendations

1.5.1. Centralized Security Awareness Training Platform

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

CSRM expanded its Security Awareness and Training service to provide a centralized solution available to all Commonwealth agencies, not just the executive branch agencies under VITA purview. This will provide a cost-effective consistent means to measure the progress of participating entities. The platform selected, KnowB4, was purchased in December 2022 for a 2023 rollout.

1.5.2. Theft or Loss of Electronic Devices

Lost or stolen physical devices accounted for the majority of the cybersecurity incidents in 2022. The prolific use of mobile phones, laptops, and tablets increases the likelihood of loss and possible loss or unauthorized disclosure of Commonwealth information.

1.5.3. Cybersecurity Attacks & Investigations

VITA detected over 55 million attempted attacks – approximately 1.75 attacks per second. CSRM supported more than 1,000 security investigations on behalf of the Commonwealth in 2022. CSRM recommends agencies identify and implement security controls to reduce the probability and impact of an exploit until security remediation patches are available and installed.

1.5.4. IT Compliance Grades

Overall IT Audit and IT Risk compliance grades declined for a second year. CSRM recommends setting interim deadlines for key deliverables throughout the year to help monitor progress.

1.5.5. Nationwide Agency Self-Evaluation

Commonwealth agencies participating in the 2022 NCSR self-assessment tend to assess their compliance with national standards at or above the minimum target score of 5.

2. Commonwealth Threat Management Report

In 2022, the Commonwealth continued to support cybersecurity programs and enhance threat management capabilities. One key measure included applying and receiving a 4-year federal grant funding for Commonwealth of Virginia cybersecurity programs to include state, local, and territorial (SLT) entities. The Virginia Cybersecurity Planning Committee (VCPC), created in November 2022, will create and approve a cybersecurity plan aligned with the grant requirements and guide the disbursement of awarded funds.

The Commonwealth also ratified legislation requiring all public bodies to report security incidents to the Virginia Fusion Center. Centralized incident reporting will help the Commonwealth identify, prioritize, and utilize threat management resources more effectively.

Cyberattacks against the Commonwealth increased by 33% in 2022. The Commonwealth experienced over 55 million attack attempts on the network and blocked more than 73,000 pieces of malware during 2022. Adding to Commonwealth's risk posture, there was a significant increase in lost or stolen devices (e.g., laptops) in 2022.

2.1.1. Virginia Cybersecurity Planning Committee (VCPC) & Cybersecurity Grant

In November 2022, the Virginia Cybersecurity Planning Committee (VCPC) was created pursuant to the Infrastructure Investment and Jobs Act (IIJA), Pub. L. No. 117-58, § 70612 (2021), and Item 93(F) of Virginia's 2022 Appropriation Act. A group of leaders from state and local government were appointed to the committee charged with several tasks, to include creating a cohesive planning network that builds and implements cybersecurity preparedness initiatives using FEMA resources, as well as other federal, state, local and tribal, private sector and faith-based community resources. This program will help the Commonwealth coordinate, prioritize and utilize cybersecurity resources more efficiently and effectively for the purpose of protecting critical infrastructure.

2.1.2. Centralized Incident Reporting – Virginia Fusion Center

To enhance Commonwealth threat intelligence and threat management capabilities, legislation requiring all public organizations to report security incidents to the Virginia Fusion Center effective July 2022. A working group was convened to ensure localities had a voice into how this legislation would be operationalized. Prior to this reporting requirement, incident information from localities or many higher education entities lead to a lack of visibility into the overall Commonwealth risks and negatively impacted the ability to determine best countermeasures.

2.2. Cybersecurity Incidents

Cybersecurity Incidents Increased 15% in 2022.

COVA networks experienced a total of 235 cybersecurity incidents in 2022. The top 3 types of incidents in 2022 were attributed to physical loss, malware, and information disclosure. The number of lost or stolen Commonwealth devices increased from 52 to 103, accounting for 43.83% of 2022 cybersecurity incidents. The number of successful malware incidents increased from 26 to 53, while the number of information disclosure incidents decreased slightly, down to 51 compared to 59 incidents in 2021.

Physical Theft or Loss of Electronic Devices Increased in 2022.

Users are not only using laptops, but they also have tablets and smartphones that allow them to check email, perform banking transactions, surf the internet, and communicate with business partners and co-workers. Given the number of devices in use across the Commonwealth, the probability of lost or stolen devices is high. Information stored or accessible via these devices may be compromised in the event of a lost or stolen device. To mitigate the risk of unauthorized disclosure or loss of Commonwealth data, it is important to implement and adhere to security controls designed to reduce the impact of lost or stolen devices (e.g., end-point security control such as encryption) and to continue to emphasize physical security in security awareness training. Physical loss incidents are attributed to users who need to be more cognizant of their surroundings and must maintain custody of their COV issued devices.

More than 73,000 Pieces of Malware Blocked in 2022.

Despite preemptive measures, 22.55% of 2022's cybersecurity incidents are attributed to malware attacks. Malware attacks remain pervasive. Increase in malware attacks in the Commonwealth also follows the cyclical patterns of on-line activity such as holiday shopping and tax season. In 2022, Commonwealth solutions blocked malware significantly.

Information Disclosure Incidents Decreased in 2022.

Information Disclosures remains a top three category for another year. This trend also highlights unauthorized disclosure of information attributed to human error and vulnerabilities. With more than 21% of the cybersecurity incidents categorized as information disclosure, efforts to remediate vulnerabilities should be allocated to remediate vulnerabilities most likely to be exploited and result in the loss of Commonwealth information.

Commonwealth Security has implemented many layers of protection to reduce the risk of information disclosure and unauthorized access. Securing data and systems goes beyond security solutions. Best practices that should be followed as part of a cybersecurity program include:

- All systems must be protected with the necessary security technology
- All systems need to be patched and/or upgraded to supported versions of software
- All systems need to be continually scanned for vulnerabilities and issues promptly remediated
- All systems should implement multi-factor authentication when possible
- Users need to be given ongoing security awareness training that includes:
    - Safe browsing habits.
    - How to identify suspicious email messages.
    - Use of email encryption.
    - What to do if something appears suspicious.
    - What not to do if something appears suspicious.
    - How to report it.

With legislative support, CSRM continues to mature the Commonwealth's security awareness training program and capabilities to provide simulated exercises. In 2022, CSRM initiated an effort to provide an

enterprise-wide security awareness training platform delivering consistent training and testing capabilities such as phishing campaigns.

Figure 1. 2022 Cyber Incidents by Category

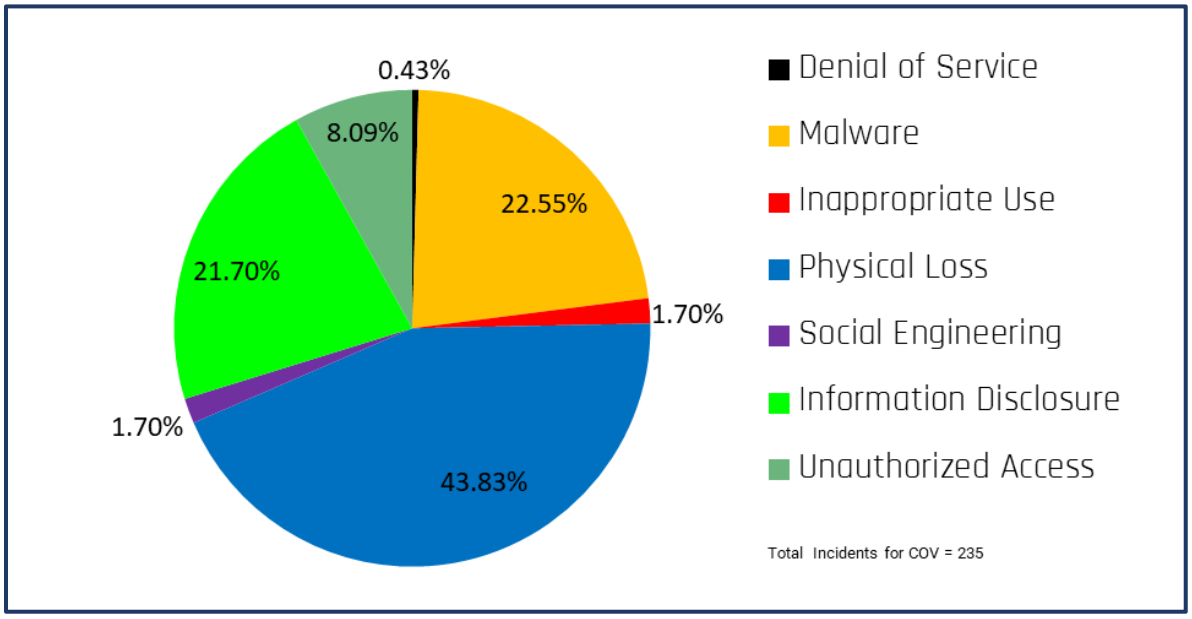


Figure 2. Malware Blocked

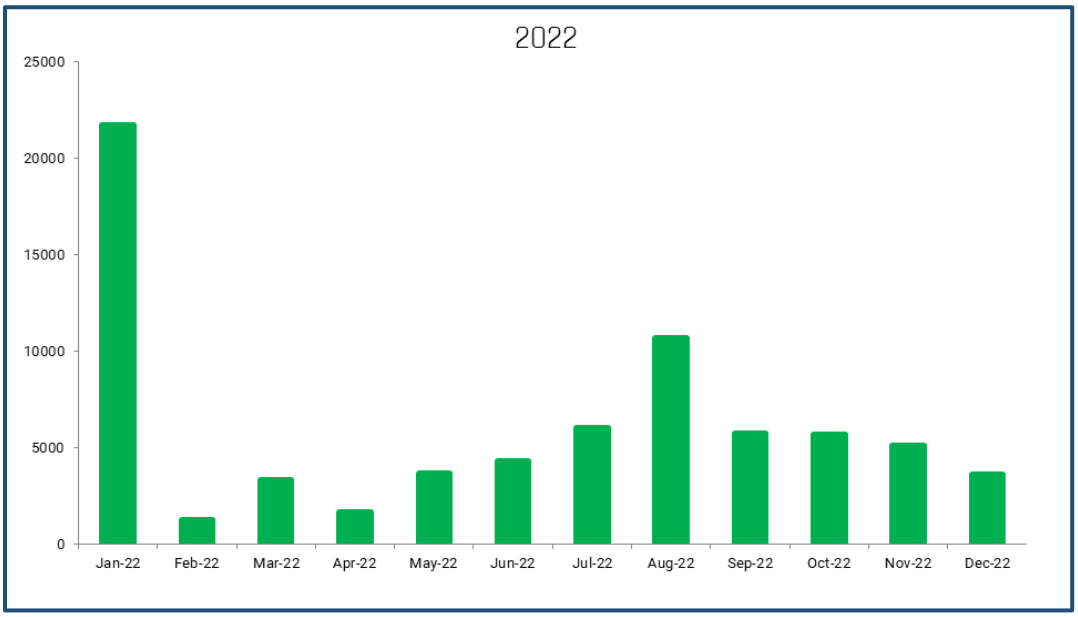
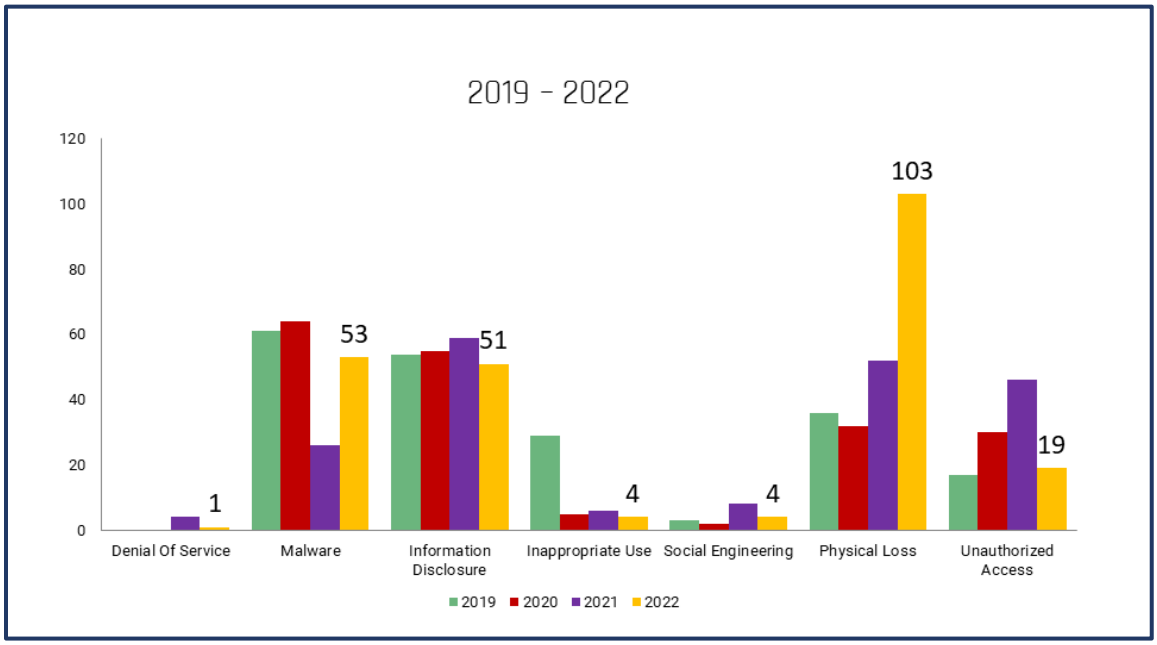


Figure 3. Historical Cyber Incident Trends

Figure 4. Historical Cyber Incident Trends by Category



2.3. Cybersecurity Attacks

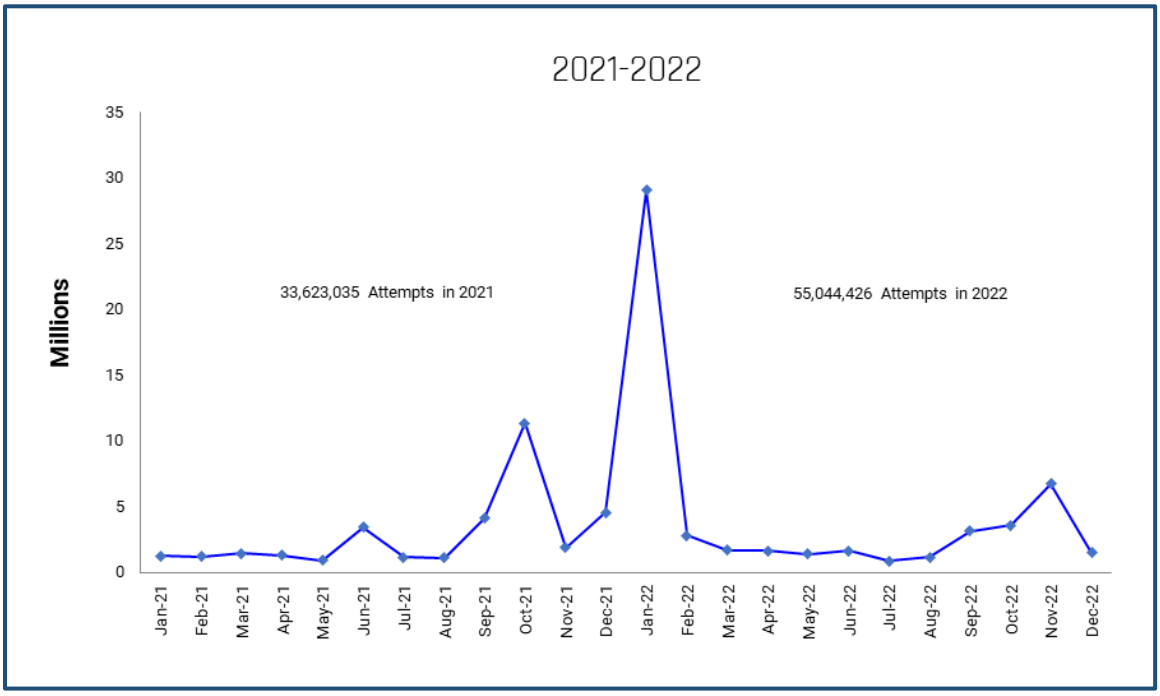
In 2022, 55 million attacks attempts were detected against Commonwealth systems – a rate of 1.75 attacks every second.

Activity spikes are indicative in new types of attack traffic being observed. When an alert is triggered, traffic activity is analyzed to determine whether it is malicious or authorized activity. Systems are adjusted to prevent malicious attack attempts from penetrating the COV network. Alerts for known authorized traffic are tuned to reduce false positive. The drop in attack attempts following a spike is due to the tuning of systems.

In 2022, most attacks on the Commonwealth originated in the United States.

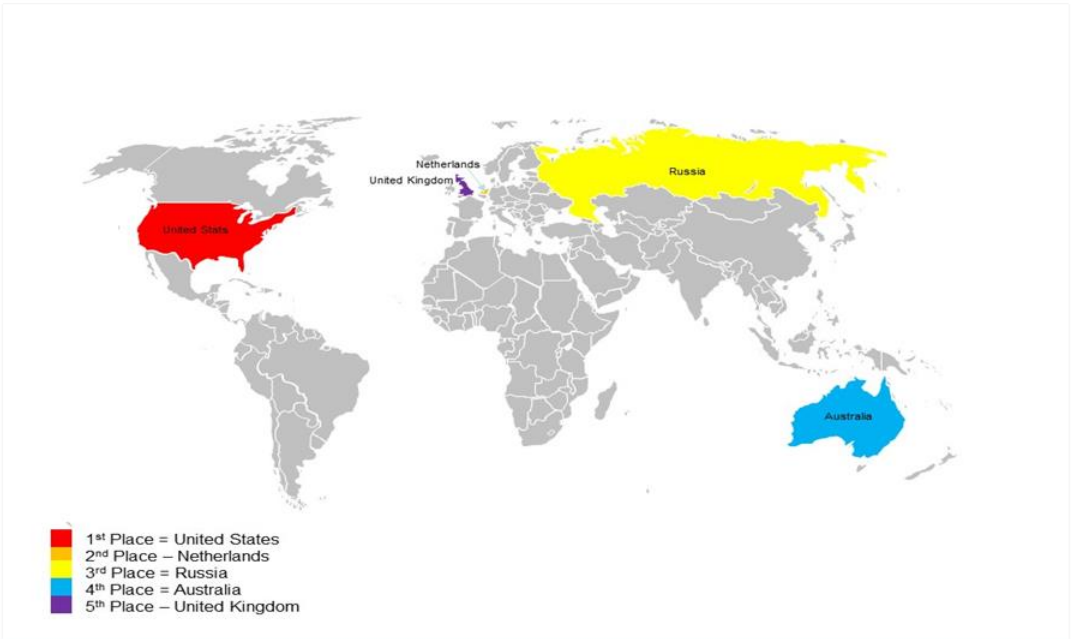
The origins of the attacks on the Commonwealth's network are monitored and tracked. CSRM receives threat intelligence information from multiple sources. This information is incorporated into the security monitoring systems that protect the Commonwealth's data from attack. We correlate this information with our intelligence partners. We then proactively block attacks from the points of origin before systems are compromised. During the past year, most attacks against the Commonwealth originated from within the United States, followed by attacks from the Netherlands, Russia, Australia, and the United Kingdom. It is important to remember that attack origination does not define attack attribution.

Figure 5. Attack Attempts on COVA Networks



The spike in January 2022 is due to a supply chain attack against SolarWinds.

Figure 6. Top Five Attack Origins



2.4. Exploits and Vulnerabilities

Critical vulnerabilities increased by 43% in 2022.

An exploit (in its noun form) is a piece of code that maliciously takes advantage of a system vulnerability. Common examples of exploits include viruses, worms, spyware, ransomware, and Trojan horses. In 2022, the number of cyber security incidents increased as new exploits and malware entered the Commonwealth's environment. Cybersecurity incident numbers decrease as counter measures, such as blocks, are provided.

CSRM identified 118,803 instances of Critical and High vulnerabilities.

The top five critical and high vulnerabilities fall into two specific categories – Remote Code Execution (RCE) and SQL Injection (SQLi). RCE vulnerabilities may be used to infiltrate a system and allow an attacker to take control of a system. Attackers use SQLi vulnerabilities to view, edit, or even download database information. CSRM recommends agencies continue to prioritize remediation for RCE and SQLi vulnerabilities. SQLi and RCE attacks are not new types of attacks, however they continue to pose risk to COV networks until related vulnerabilities are remediated.

SQL Injection (SQLi) allows an attacker to access unauthorized data in a SQL database using dynamic queries and unvalidated user input.

This common attack vector uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details. When an SQLi attack occurs, the vendor/developer must remediate the vulnerability and database administrators must validate the data in the database. Data breach notifications may be required.

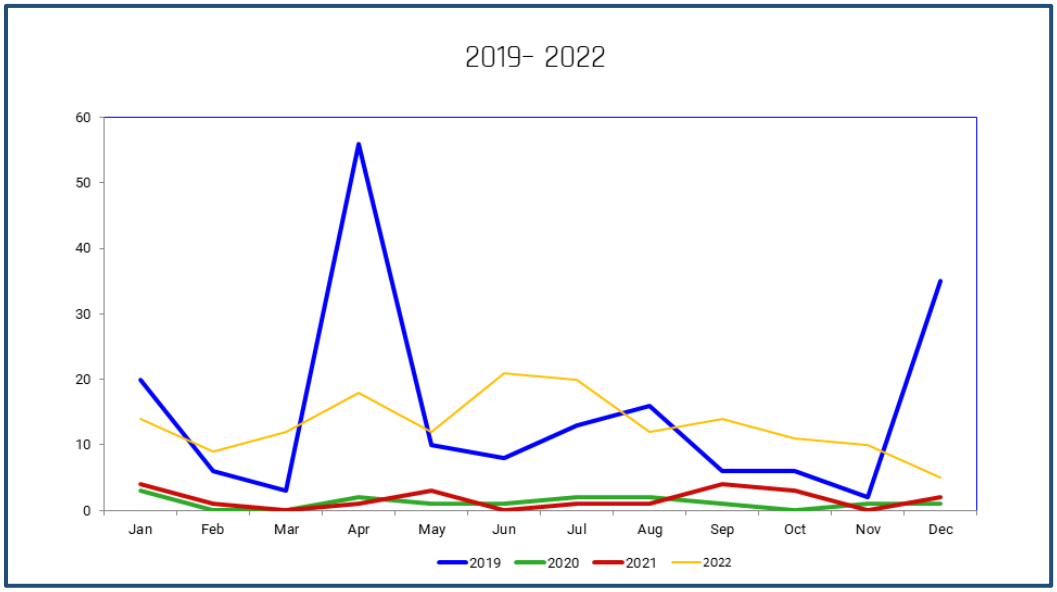
Remote Code Execution (RCE) allows an attacker to execute any command or application of their choosing.

Attackers may use RCE vulnerabilities to install malware, escalate their privileges and to maintain persistence into the system. Because RCE does not require physical access to the system, the victim may be unaware that a compromise has occurred. Once a system has been compromised through an RCE vulnerability, the system must be rebuilt. RCE vulnerabilities are very serious; they provide an attacker full access to the system. RCE vulnerabilities can be remediated by applying patches in a timely manner.

CSRM recommends implementation of mitigation controls to reduce the probability and impact of an exploit until security patches are made available for remediation.

Because system vulnerabilities provide attackers with advantages, is important to identify and prioritize system vulnerabilities together with appropriate remediation efforts. Common remediation efforts may include installing and applying system patches and updates, updating system communication protocols, or changing custom code. "Zero-day" vulnerabilities are unknown errors, typically discovered by malicious attackers.

Figure 7. Critical Vulnerabilities Yearly Trend



2.5. Commonwealth Web Applications

CSRM Threat Management team conducted 11,127 scans of external websites in 2022.

These scans were conducted on a quarterly basis. Vulnerabilities with a High or Medium severity were tracked. During the first quarter of 2022, we saw a spike in web application vulnerabilities. This was due to many applications utilizing vulnerable java script libraries, being vulnerable to cross site scripting and HTTP parameters pollution attacks.

Cross-Site Scripting (XSS) was the most prevalent web application vulnerability ranked with a High severity level.

Cross-site scripting is where an attacker can execute a client-side script by embedding it in a web page. Since the browser has no way of knowing this doesn't belong there, it executes the script. This allows the user to be vulnerable to account impersonation, stealing sensitive data as well as other types of attacks. The vulnerabilities can be corrected by performing input validation and sanitization on all variables used in the application.

SQLi vulnerabilities were also among the top web application vulnerabilities in 2022.

SQL injection (SQLi) allows an attacker to manipulate a database by entering SQL commands in a query. When this occurs, the attacker can steal sensitive data, replace, or add invalid data to the database and can even delete data from the database. This vulnerability can be resolved by using prepared statements with parameterized queries, using stored procedures, implementing allow-lists for input validation, and escaping all user-supplied input. Using strict controls around what data can be submitted will prevent SQL injection vulnerabilities.

Javascript library flaws topped the 2022 list of web application vulnerabilities with a Medium severity level.

Unsecure encryption protocols and ciphers also topped the list of medium web application vulnerabilities. While not as severe as high vulnerabilities, exploitation of medium vulnerabilities can be used to gather information about systems or to compromise a user's session.

These vulnerabilities can be resolved by:

- Updating software
- Configuring systems to use secure protocols and ciphers
- Limiting access to application error messages to internal users

Figure 8. Web Application Exploits by Quarter

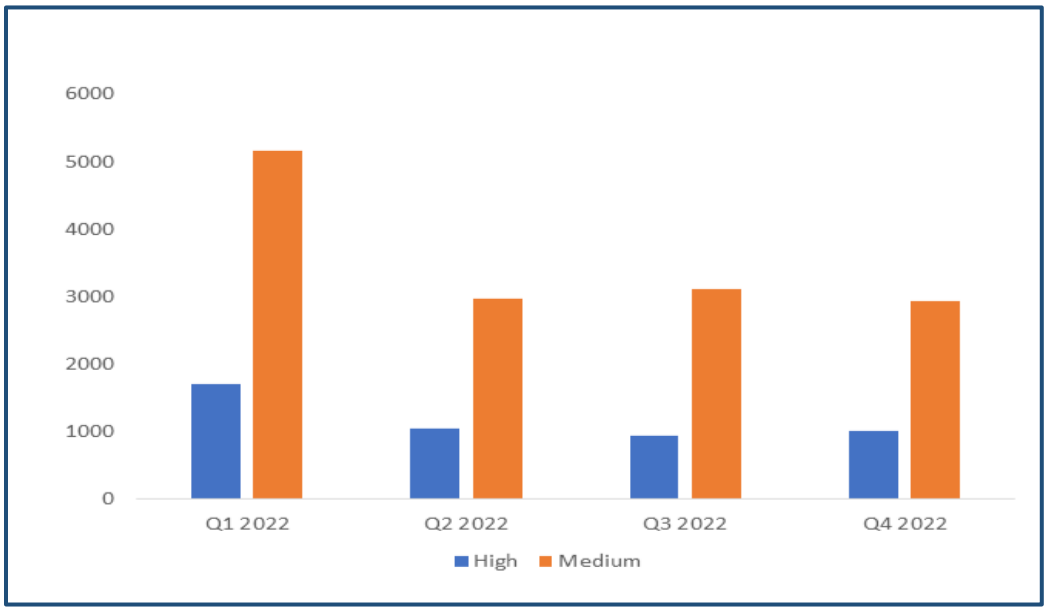


Figure 9. Top Five High Web Application Vulnerabilities

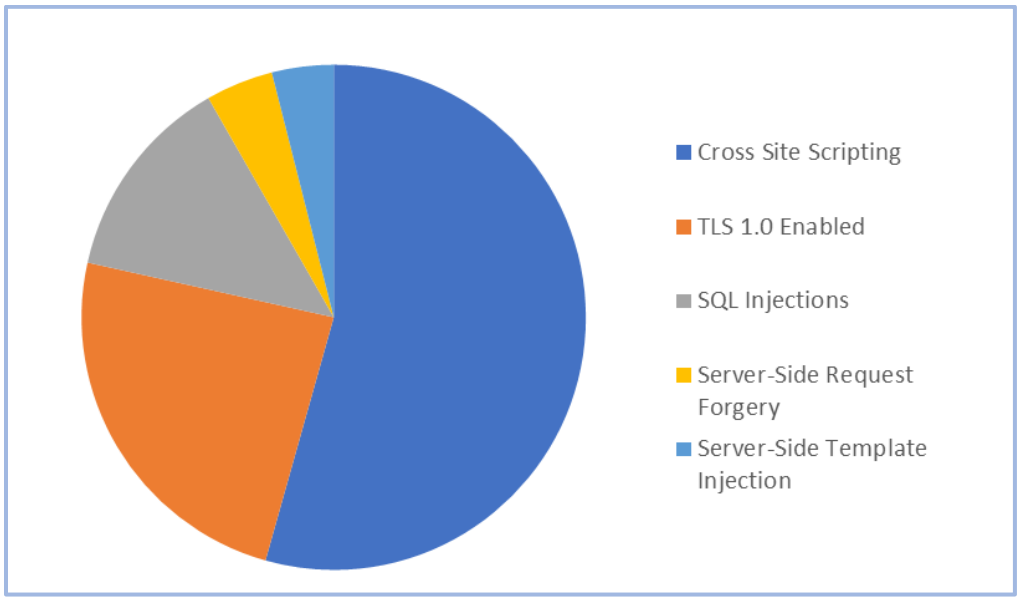
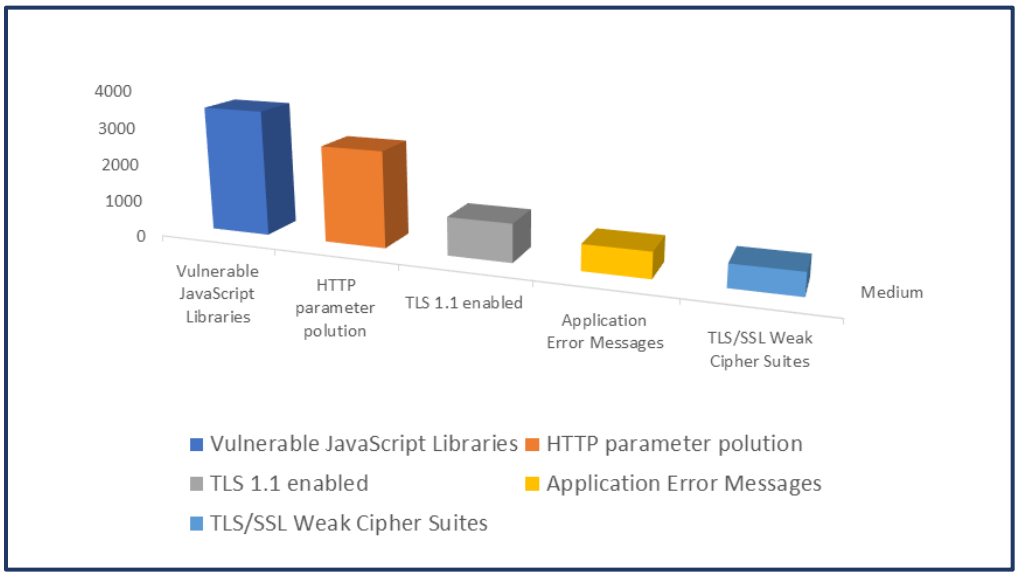


Figure 10. Top Five Medium Web Application Vulnerabilities



2.6. Security Investigations

Information received from Commonwealth partners includes data involving state and local governments, higher education institutions, and public-school systems. MS-ISAC compiles data by monitoring the internet for potential events. 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 11. Security Investigations by Entity

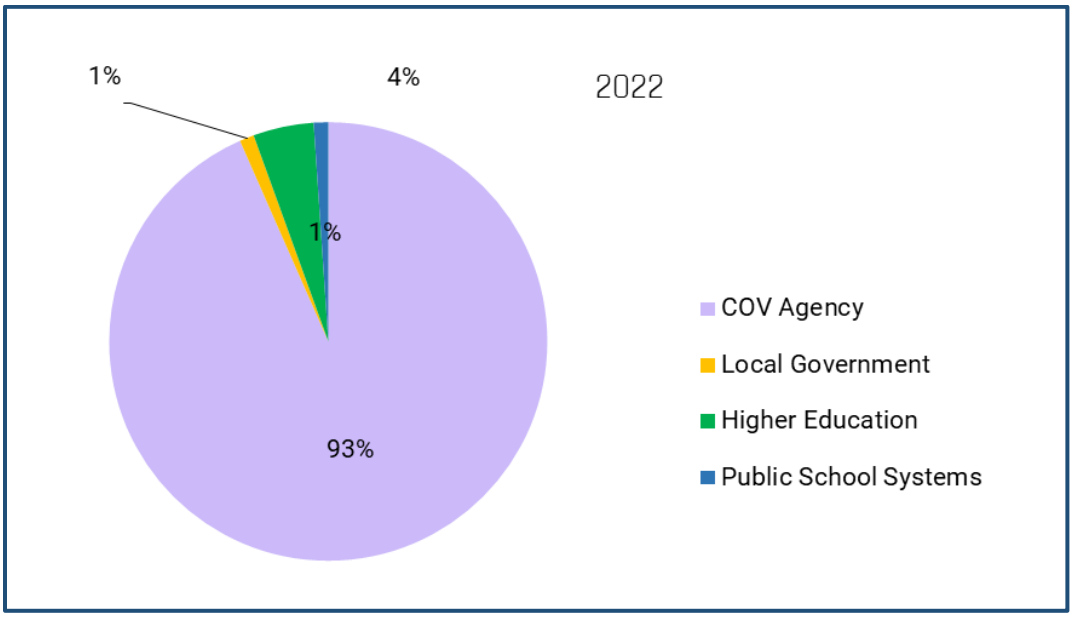
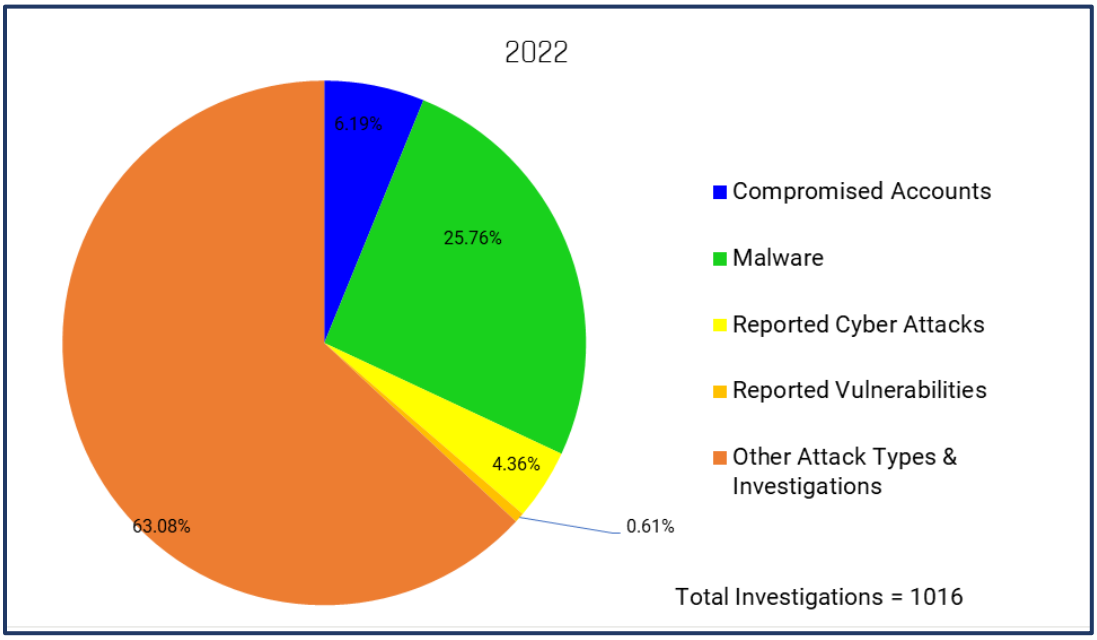


Figure 12. Security Investigations by Category



3. 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.

3.1. 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 19 information security risk program standards and policies. CSRM continues its transition toward a level that provides additional insight into agency programs and will enable the Commonwealth to improve security endeavors.

3.2. Security Awareness Training and Phishing Campaigns

CSRM sponsored a project to implement an enterprise-wide security awareness training platform to provide consistent training opportunities to Commonwealth users.

User training is paramount to the protection of publicly owned assets. In 2022, 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. This will provide a more cost-effective solution and introduces a consistent way to measure progress of participating entities. The platform selected, KnowBe4, was purchased in December 2022 for a 2023 rollout.

Using the latest threat intelligence, the CSRM Threat Management 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. Despite a slight dip in the pass rate during the second quarter campaign, pass rates climbed in the third and fourth quarter of 2022.

3.3. 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. Due to the pandemic, 2022 courses remained virtual. To help agency ISOs satisfy certification requirements, CSRM plans to offer the course more frequently and in-person. 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.

3.4. 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. While all ISOAG meetings in 2022 remained virtual, CSRM anticipates adding in-person meetings in 2023.

3.5. 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 get agency input as we work to develop practical and effective security initiatives.

3.6. IT Risk Management Committee

The IT Risk Management Committee is made up of risk specialists from CSRM's IT Risk Management division and with 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.

3.7. 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 multi-sourcing integration (MSI) model identifying cybersecurity risks and tracking 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 has established a security review process for third party systems and services to ensure those services are secure, dependable and resilient. The Enterprise Cloud Oversight Service (ECOS) is a service specifically created for establishing contract term and oversight of third-party vendors offering Software as a Service (SaaS) 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 in place prior to being implemented.

3.8. 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.

3.8.1. 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.

3.8.2. Shared ISO Service

In 2022, 37 customer agencies subscribed to the ISO service, up from 26 subscriptions in 2021. 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.

3.8.3. 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.

3.9. 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.

3.9.1. 2022 IT Audit and Risk Compliance and Grades

In 2022, 36% of IT Audit compliance grades were above average.

While 36% of the IT audit compliance grades were above average, the percentage of failing grades increased to 32%. CSRM attributes this to a decline in the number of IT audits performed in 2022. CSRM anticipates audit program compliance will improve as agencies plan to complete required audits.

In 2022, 47% of IT Risk compliance grades were above average.

Overall IT risk compliance declined – 53% of the risk compliance grades were at or below average. Many risk grades could have improved by a letter grade if the Risk Assessment Plan requirement had been satisfied. The risk assessment plan lists an agency's sensitive systems and planned calendar year to complete a risk assessment.

Figure 13. 2019 – 2022 Audit Compliance Grades

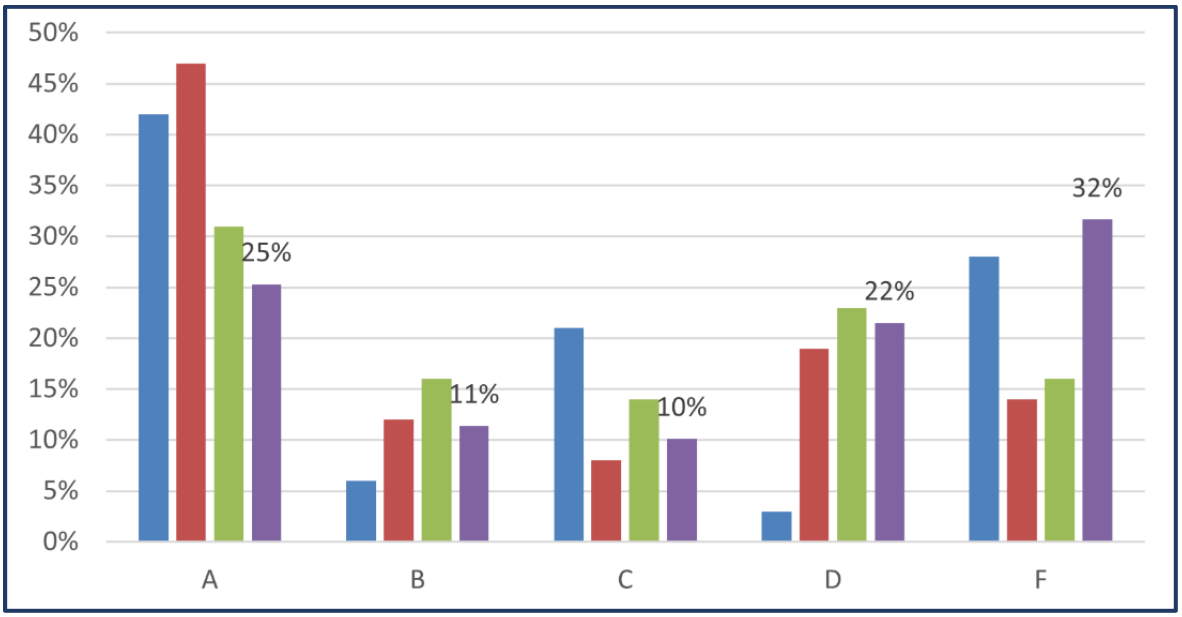


Figure 14. 2019 – 2022 Risk Compliance Grades

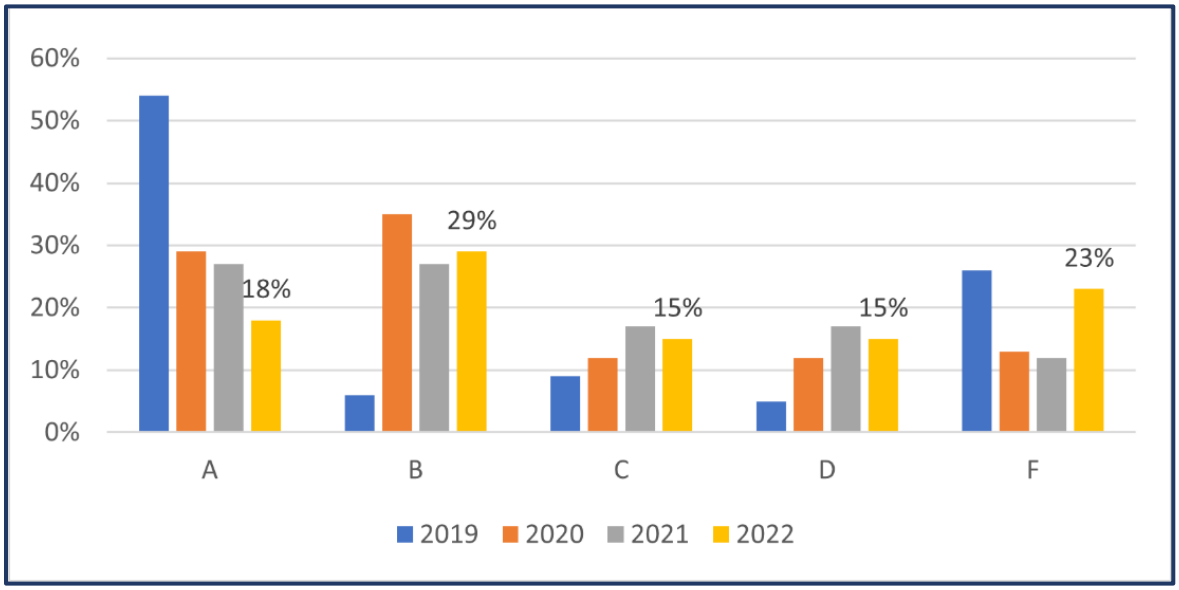


Table 1. 2022 IT Audit & Risk Compliance Analysis

Program	Metric	Full Compliance Rate	1 Year Change	Notes
Audit	Audit Plan	82%	8% Decrease	
	3 Year Audit Obligation	18%	Same	
	Current Year Percentage of Quarterly Findings Updates Received: Audit	61%	23% Decrease	13% partial compliance
Risk	Risk Assessment Plan	75%	14% Increase	
	3 Year IT Risk Assessment Obligation	13%	14% Decrease	
	Business Impact Analysis (BIA) Status	80%	3% Increase	7% partial compliance
	Current Year Percentage of Quarterly Findings Updates Received: IT risk assessments	38%	26% Decrease	68% partial compliance
	Quarterly Intrusion Detection Systems (IDS) reports are received	91%		
	Applications Certified	87%	3% Decrease	3% partial compliance
	ISO Certification Status	78%	6% Decrease	
	ISO Reports to Agency Head	81%	2% Increase	

3.9.2. 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 2022, CSRM reports the average age for all open IT audit and risk findings is 807 and 1,240 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, 29% 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 15. 2022 Findings by Secretariat

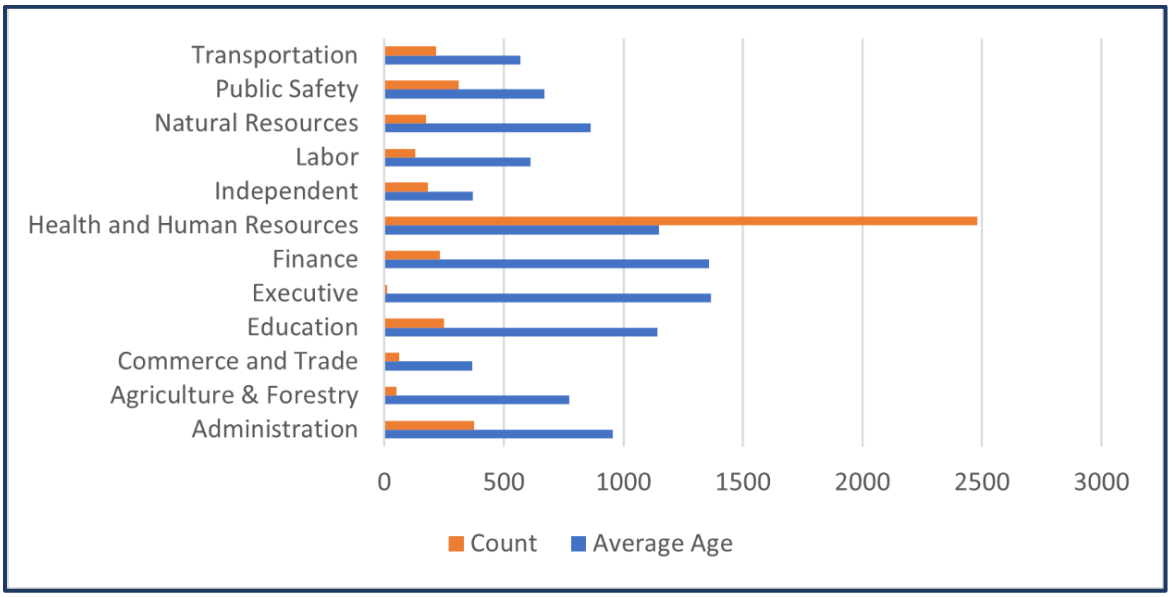


Figure 16. 2022 Audit Findings By Security Control Family

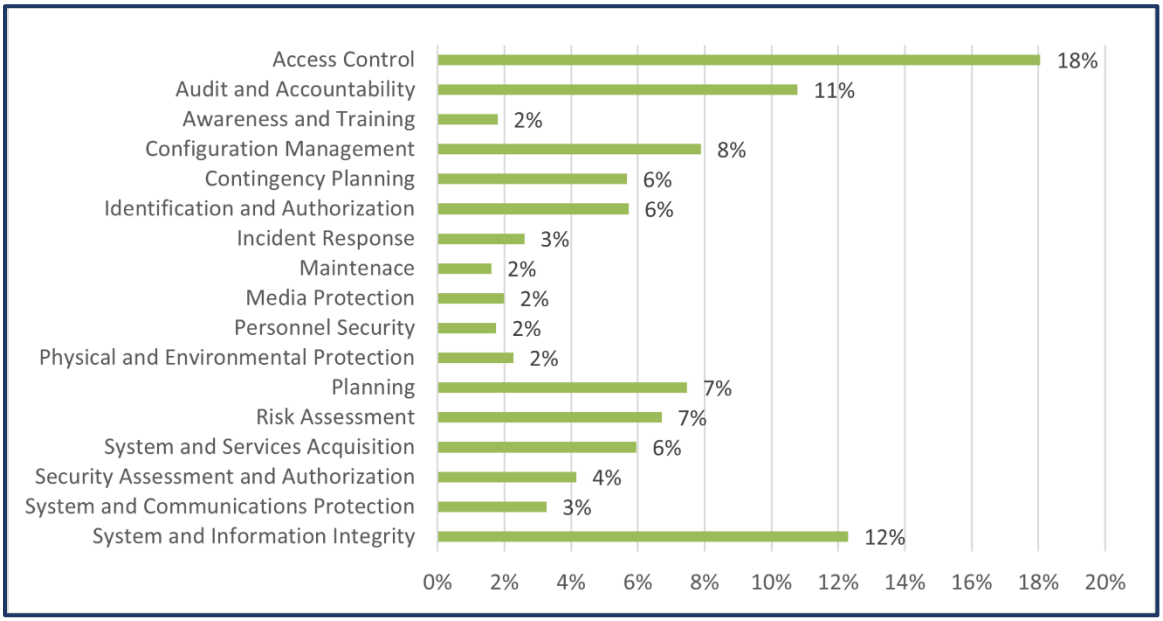
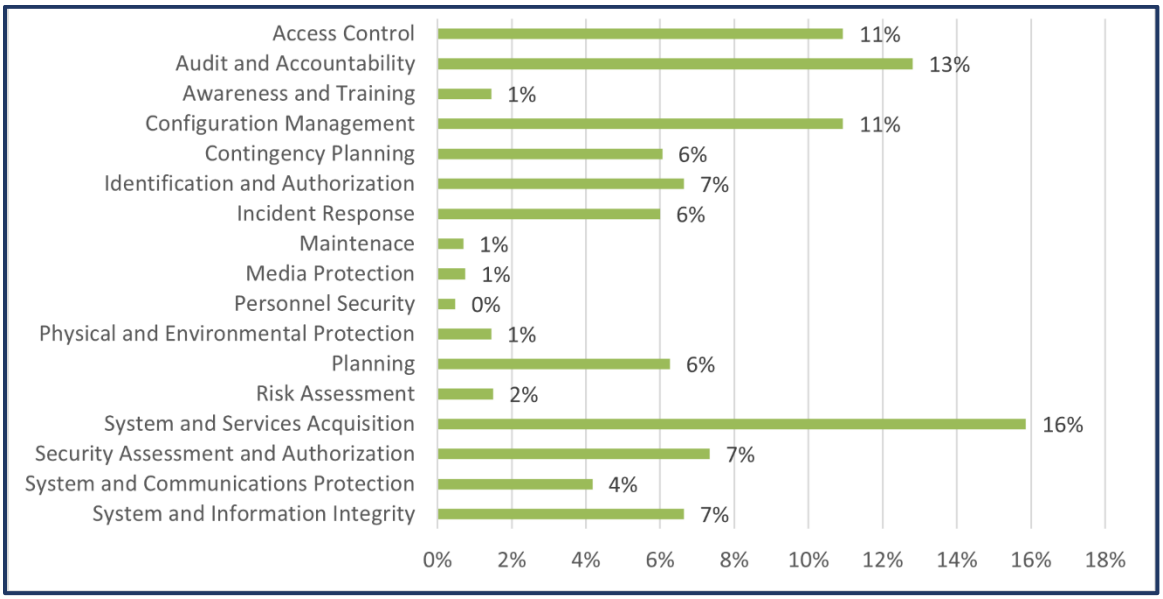


Figure 17. 2022 Risk Findings By Security Control Family



4. Nation-wide Cybersecurity Review (NCSR) Assessment

4.1. 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 by-annually 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, 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.

4.2. 2022 Assessment Summary

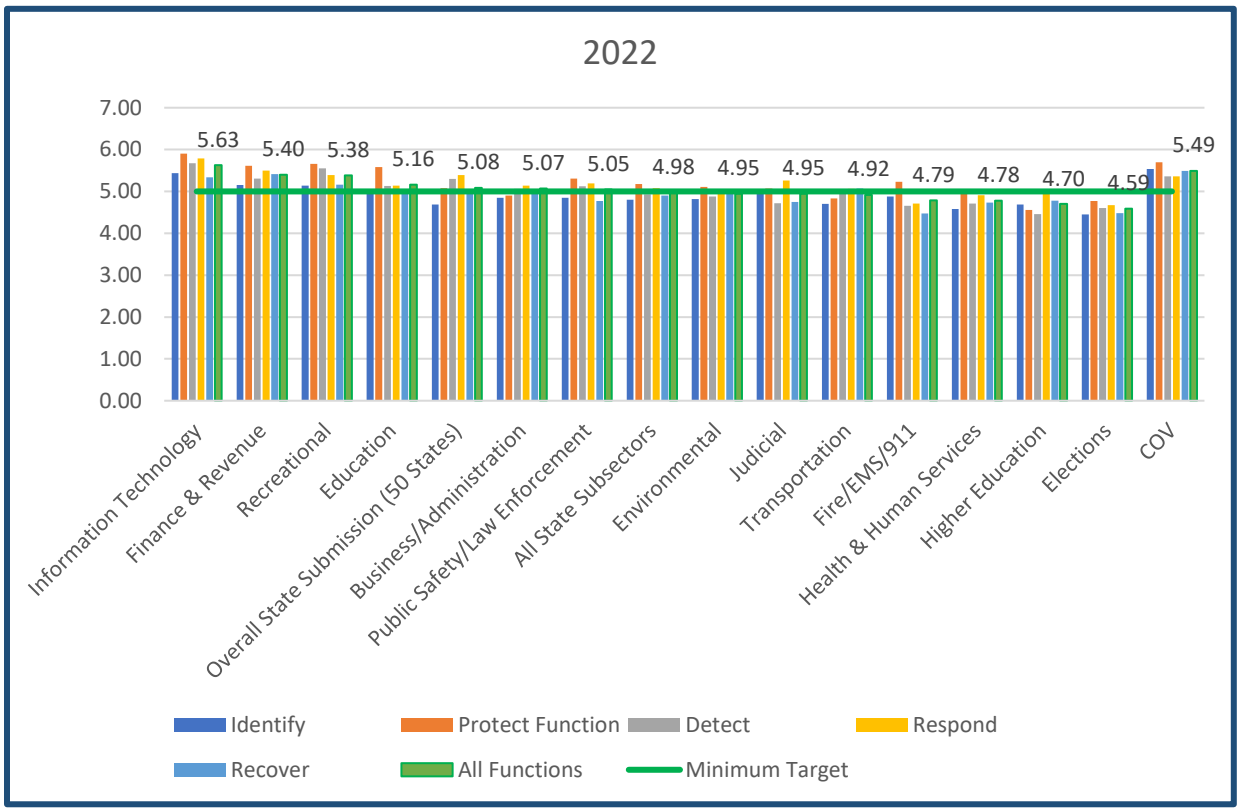
In 2022, 39 Commonwealth agencies participated in the NCSR assessment and reported overall increases in maturity scores. The Commonwealth reports slightly higher scores than peer states, continues to trend higher in the identify and protect functional areas, and reports more conservative scores in the 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.

4.3. Peer Assessment

In 2022, the average maturity score for CSF functions for the Commonwealth is 5.49 (on a 7-point scale), an increase from 5.15 in 2021.

The overall average for participating states submissions is 5.08. 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. Information technology and finance sub sectors report higher maturity scores, while higher education and elections report lower maturity scores. Functionally, participating Commonwealth agencies rank themselves more mature in the protect function and lower maturity scores in the Detect function.

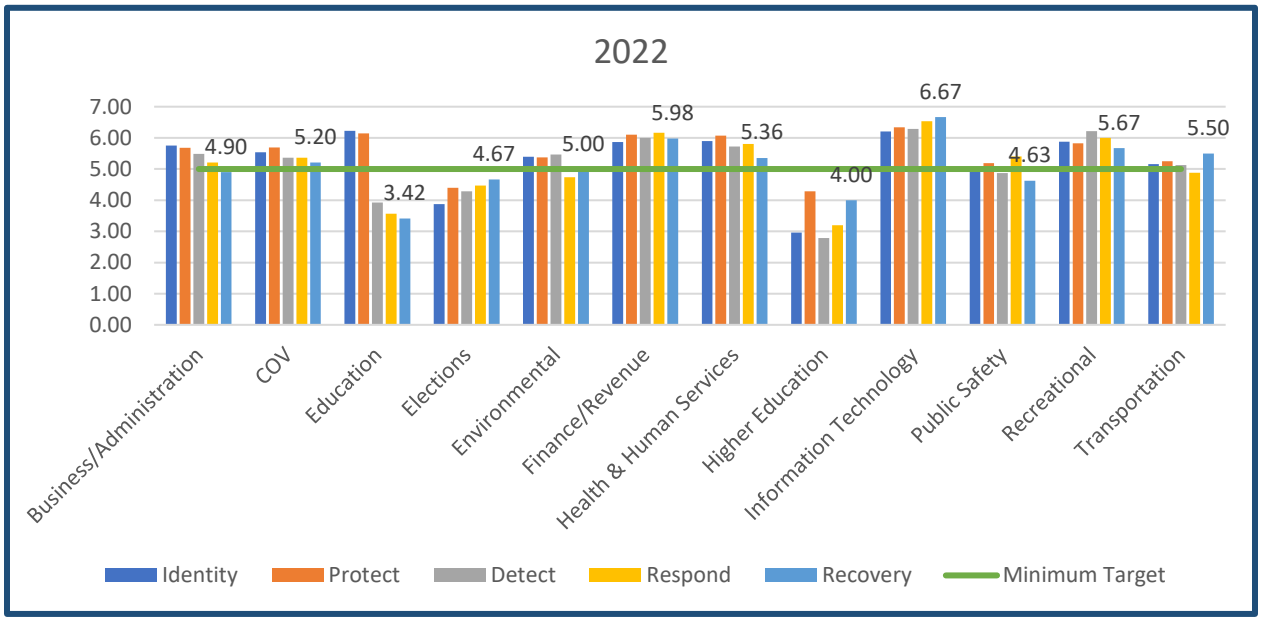
Figure 18. Commonwealth (COV) compared to state Peers and Sub -Sectors



4.4. Commonwealth Self-Assessment

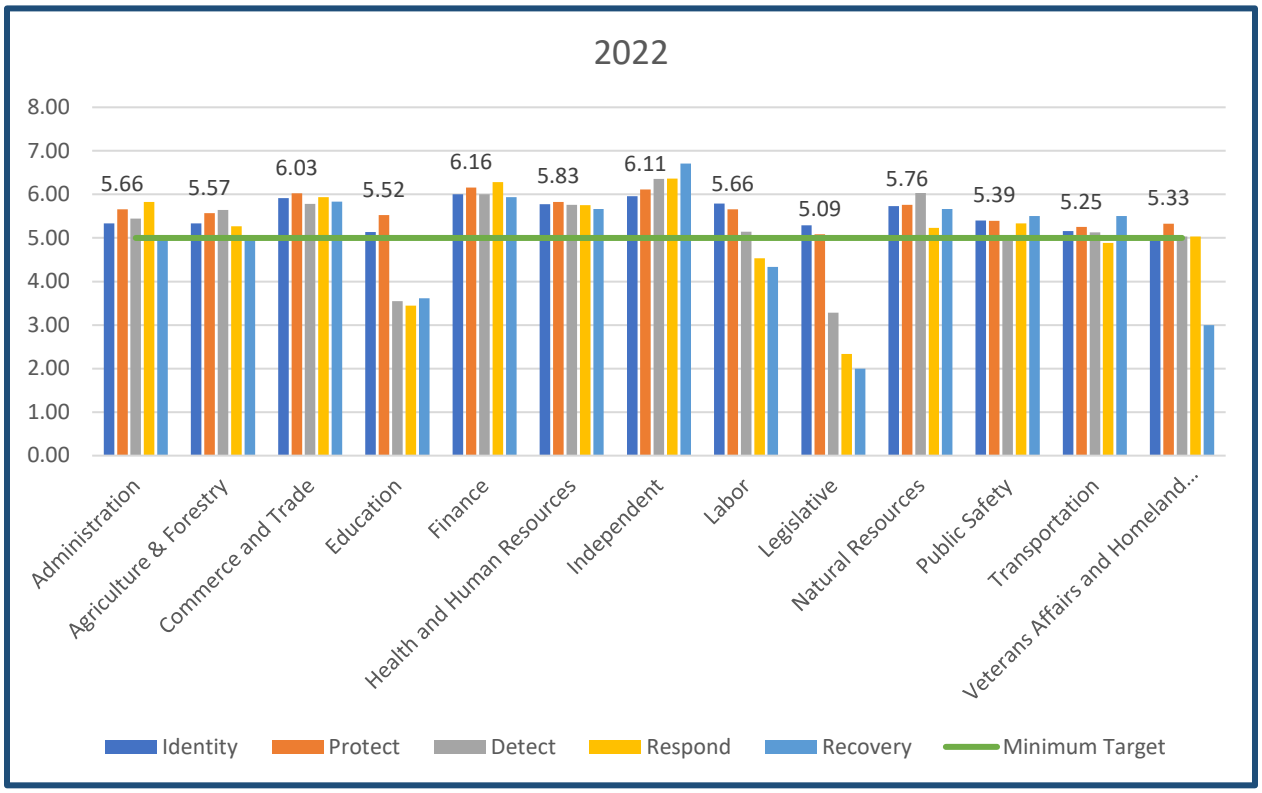
In 2022, the Commonwealth's information technology and finance subsectors report higher maturity scores. Commonwealth education and higher education organizations report lower maturity scores. Commonwealth (COV) agencies by sub sector.

Figure 19. Commonwealth (COV) Agencies by Sub-Sector



All Secretariats report assess at least one functional area meeting the recommended maturity level of 5. Agencies report lower scores in the Detect, Respond, and Recovery functions.

Figure 20. Commonwealth (COV) Agencies 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.

Table 2. 2022 NCSR Self-Scoring Results

Function	Categories	Maturity Level	COV Averages
Identify	Asset Management	Implementation in Process	5.6
	Business Environment	Implementation in Process	5.46
	Governance	Implementation in Process	5.71
	Risk Assessment	Implementation in Process	5.6
	Risk Management Strategy	Implementation in Process	5.19
Protect	Access Control	Tested and verified	6.11
	Awareness and Training	Implementation in Process	5.89
	Data Security*	Implementation in Process	5.70
	Information Protection Processes and Procedures	Implementation in Process	5.58
	Maintenance	Implementation in Process	5.37
	Protective Technology	Implementation in Process	5.31
Detect	Anomalies and Events	Implementation in Process	5.2
	Continuous Monitoring	Implementation in Process	5.42
	Detection Processes	Partially Documented Standards and/or Procedures	4.83
Respond	Analysis	Implementation in Process	5.63
	Communications	Implementation in Process	5.45
	Improvements	Implementation in Process	5.32
	Mitigation	Implementation in Process	5.36
	Response Planning	Implementation in Process	5.10
Recover	Communications	Implementation in Process	5.21
	Improvements	Implementation in Process	5.01
	Recovery Planning	Implementation in Process	5.33

Appendix I. 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
	3 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
	3 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 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 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" are 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 & 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. Agency Information Security Data Points

Legend

Audit plan status
Pass - Documents received as scheduled
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

IDS (intrusion detection system) quarterly reports
Pass - Documents received as scheduled
N/C - Reports were not received

Applications Certified
Compliant – Agency application inventory is compliant for completeness
Non-Compliant – 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 report to Agency Head
Yes - Agency ISO reports to Agency Head
No - Agency ISO does not report directly to Agency Head

Agency Name	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	BIA Status	Current Year Percentage of Risk Finding	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	Agency Secretariat
Department for Aging and Rehabilitative Services	Pass	83.00%	60.44%	Pass	0%	0.98	91.49%	Pass	Compliant	Pass	Yes	Health and Human Resources
Department for the Deaf and Hard of Hearing	Pass	100.00%	N/A	N/C	N/C	1	96.59%	Pass	Compliant	Pass	Yes	Health and Human Resources
Department of Aviation	Pass	75.00%	76.92%	Pass	0.5	1	77.27%	Pass	Compliant	Pass	Yes	Transportation
Department of Corrections	Pass	87.00%	94.89%	Pass	0.4	1	99.38%	Pass	Compliant	Pass	Yes	Public Safety
Department of Forestry	Pass	60.00%	31.15%	Pass	N/C	1	50%	Pass	Compliant	Pass	No	Agriculture & Forestry
Department of General Services	Pass	0.00%	27.27%	N/C	N/C	1	25.00%	Pass	Compliant	Pass	Yes	Administration
Department of Human Resource Management	Pass	62.00%	100.00%	Pass	88%	1	50%	Pass	Compliant	Pass	Yes	Administration
Department of Medical Assistance Services	Pass	29.06%	100.00%	Pass	2%	1	87.95%	Pass	Compliant	Pass	Yes	Health and Human Resources
Department of Professional and Occupational Regulation	Pass	0.00%	N/A	Pass	33%	1	25.00%	Pass	Compliant	Pass	Yes	Labor
Department of Social Services	Pass	19.00%	0%	N/C	N/C	0.96	7.44%	Pass	Compliant	Pass	Yes	Health and Human Resources
Department of Taxation	Pass	49.00%	61.36%	Pass	79%	1	78.52%	Pass	Non-Compliant	Pass	Yes	Finance

Agency Name	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	BIA Status	Current Year Percentage of Risk Finding	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	Agency Secretariat
Gunston Hall	Pass	0.00%	N/A	Pass	75%	1	25%	Pass	Compliant	Pass	Yes	Education
Office for Children's Services	Pass	75.00%	33.33%	Pass	N/C	1	88%	Pass	Compliant	Pass	Yes	Health and Human Resources
State Corporation Commission	Pass	62.00%	60.58%	Pass	77%	1	66.67%	Pass	Compliant	Pass	Yes	Independent
Virginia Department of Agriculture and Consumer Services	Pass	95.00%	100%	Pass	0%	1	50%	Pass	Compliant	Pass	Yes	Agriculture & Forestry
Virginia Department of Transportation	Pass	65.00%	100.00%	N/C	N/C	1	25%	Pass	Compliant	Pass	No	Transportation
Virginia Employment Commission	Pass	50.00%	30.10%	Pass	50%	1	60.61%	Pass	Compliant	Pass	Yes	Labor
Virginia Information Technologies Agency	Pass	80.00%	100%	Pass	55%	1	77.48%	Pass	Compliant	Pass	Yes	Administration
Virginia Racing Commission	Pass	25.00%	100.00%	Pass	0.75	1	75%	Pass	Compliant	Pass	Yes	Agriculture & Forestry
Virginia Retirement System	Pass	100.00%	100.00%	Pass	0.8	1	40.91%	Pass	Compliant	Pass	Yes	Independent

Appendix V. Glossary & Terms

Term	Expansion
AISN	AIS Network
BIA	Business Impact Analysis
CIO	Chief Information Officer
CIS	Center for Information Security
CISC	Commonwealth Information Security Council
COV	Commonwealth of Virginia
COVITS	Commonwealth of Virginia Innovative Technology Symposium
CSF	Cyber Security Framework (NIST)
CSRM	Commonwealth Security and Risk Management
DoS / DDoS	Denial of Service / Distributed Denial of Service - Attempt to overwhelm a targeted server with a flood of internet traffic
ECOS	Enterprise Cloud Oversight Service
EoL	(Software) End of Life
Interactive	Virginia Interactive
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
Inappropriate Usage	Misuse of COV resources
Information Disclosure	COV data exposure to recipients who are not authorized to access and use the data.
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
MEF	Mission Essential Function
MS-IAC	Multi-State Information Assistance Center
NIST	National Institute of Standards and Technology
ORI	Operational Risk & Issue
PBF	Primary Business Function
Physical Loss	Loss or theft of any COV resource that contains COV data
Ponemon	The Ponemon Institute, created in 2002, is dedicated to two principles: studying information security and privacy issues and educating people about those results and their implications.
RCE	Remote Code Execution
RFI	Remote File Inclusion
RPO	Recovery Point Objectives
RTO	Recovery Time Objective

Term	Expansion
SaaS	Software as a Service
SEC501	Information Security Standard 501 (Security Awareness and Training Policy)
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
SSRF	Server-side Request Forgery
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