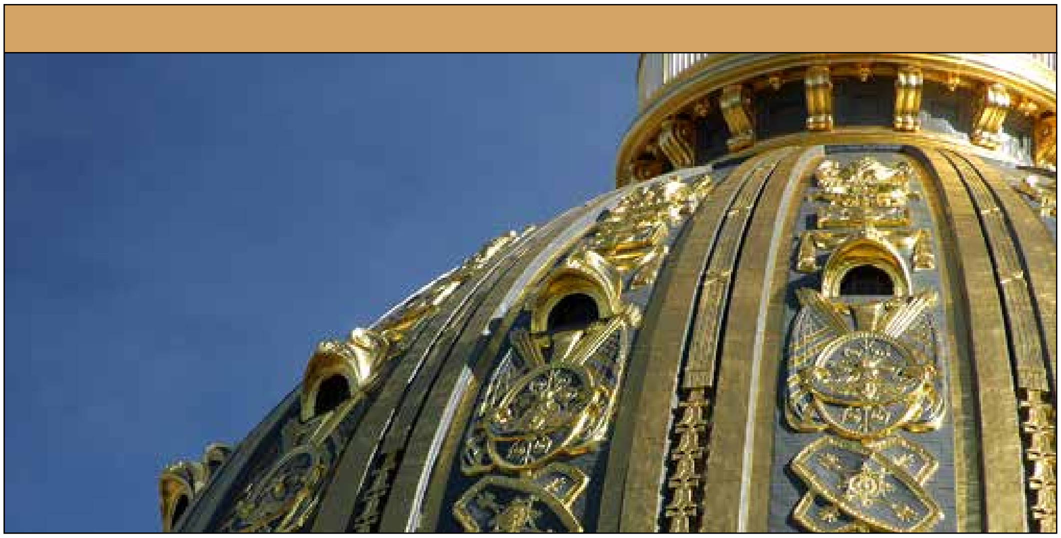


January 2026
PE 25-04-688

PERFORMANCE REVIEW

THE WEST VIRGINIA OFFICE OF TECHNOLOGY

AUDIT OVERVIEW

The West Virginia Cybersecurity Office Has Not Fulfilled the Legislative Mandate of Developing a Statewide Cybersecurity Program

WEST VIRGINIA OFFICE OF THE LEGISLATIVE AUDITOR
PERFORMANCE EVALUATION & RESEARCH DIVISION

JOINT COMMITTEE ON GOVERNMENT ORGANIZATION

Senate	House of Delegates
Patricia Puertas Rucker, Chair	Chris Phillips, Chair
Jason Barrett	Doug Smith, Vice Chair
Laura Wakim Chapman	Stanley Adkins
Anne B. Charnock	Eric Brooks
Bill Hamilton	Ryan Browning
Brian Helton	Adam Burkhammer
Glenn Jeffries	Jarred Cannon
Mark Maynard	Wayne Clark
Rupie Phillips	Marshall Clay
Chris Rose	Mark Dean
Darren Thorne	Michael DeVault
Tom Willis	Dana Ferrell
Jack Woodrum	Dave Foggin
Mike Woelfel	John Paul Hott
	Tresa Howell
	Jonathan Kyle
	Tristan Leavitt
	Patrick Lucas
	David McCormick
	Jonathan Pinson
	Charles Sheedy
	Bryan Smith
	George Street
	Kayla Young

WEST VIRGINIA OFFICE OF THE LEGISLATIVE AUDITOR

PERFORMANCE EVALUATION & RESEARCH DIVISION

Building 1, Room W-314
State Capitol Complex
Charleston, West Virginia 25305
(304) 347-4890

Justin Robinson	John Sylvia	Christopher F. Carney	Austin Barnett	Andrew Holt
Legislative Auditor	Director	Research Manager	Research Analyst	Referencer

WEST VIRGINIA LEGISLATURE
Performance Evaluation and Research Division

1900 Kanawha Blvd. East
Building 1, Room W-314
Charleston, WV 25305-0610
(304) 347-4890

John Sylvia
Director

January 12, 2026

The Honorable Patricia Puertas Rucker, Chair
State Senate
Building 1, Room 214W
1900 Kanawha Boulevard, East
Charleston, West Virginia 25305

The Honorable Chris Phillips, Co-Chair
House of Delegates
Building 1, Room 213E
1900 Kanawha Boulevard, East
Charleston, West Virginia 25305

Dear Chairs:

Pursuant to the West Virginia Performance Review Act, we are transmitting a Performance Review of the *West Virginia Office of Technology*. The issue covered herein is:

1. The West Virginia Cybersecurity Office Has Not Fulfilled the Legislative Mandate of Developing a Statewide Cybersecurity Program

We transmitted a draft copy of the report to the Office on July 24, 2025. We held an exit conference on July 31, 2025. We received the agency's written response on September 30, 2025. If you have any inquiries on this report, please let me know.

Sincerely,
John Sylvia
John Sylvia

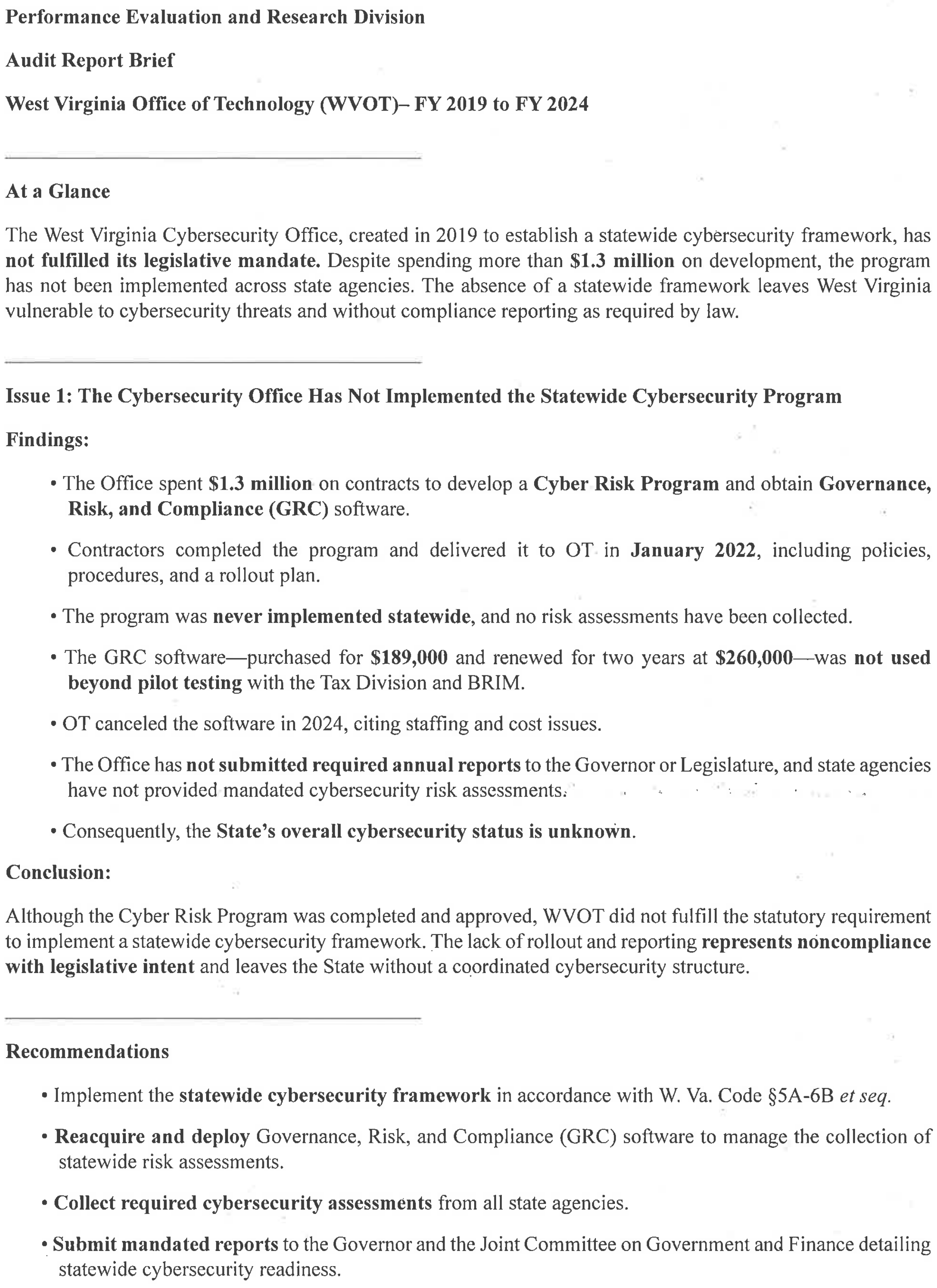
CONTENTS

List of Tables

List of Figures

List of Appendices

AUDIT REPORT BRIEF



Performance Evaluation and Research Division

Audit Report Brief

West Virginia Office of Technology (WVOT)– FY 2019 to FY 2024

At a Glance

The West Virginia Cybersecurity Office, created in 2019 to establish a statewide cybersecurity framework, has **not fulfilled its legislative mandate.** Despite spending more than **$1.3 million** on development, the program has not been implemented across state agencies. The absence of a statewide framework leaves West Virginia vulnerable to cybersecurity threats and without compliance reporting as required by law.

Issue 1: The Cybersecurity Office Has Not Implemented the Statewide Cybersecurity Program

Findings:

- The Office spent **$1.3 million** on contracts to develop a **Cyber Risk Program** and obtain **Governance, Risk, and Compliance (GRC)** software.
- Contractors completed the program and delivered it to OT in **January 2022**, including policies, procedures, and a rollout plan.
- The program was **never implemented statewide**, and no risk assessments have been collected.
- The GRC software—purchased for **$189,000** and renewed for two years at **$260,000**—was **not used beyond pilot testing** with the Tax Division and BRIM.
- OT canceled the software in 2024, citing staffing and cost issues.
- The Office has **not submitted required annual reports** to the Governor or Legislature, and state agencies have not provided mandated cybersecurity risk assessments.
- Consequently, the **State's overall cybersecurity status is unknown**.

Conclusion:

Although the Cyber Risk Program was completed and approved, WVOT did not fulfill the statutory requirement to implement a statewide cybersecurity framework. The lack of rollout and reporting **represents noncompliance with legislative intent** and leaves the State without a coordinated cybersecurity structure.

Recommendations

- Implement the **statewide cybersecurity framework** in accordance with W. Va. Code §5A-6B *et seq.*
- **Reacquire and deploy** Governance, Risk, and Compliance (GRC) software to manage the collection of statewide risk assessments.
- **Collect required cybersecurity assessments** from all state agencies.
- **Submit mandated reports** to the Governor and the Joint Committee on Government and Finance detailing statewide cybersecurity readiness.

EXECUTIVE SUMMARY

The Performance Evaluation and Research Division (PERD) within the Office of the Legislative Auditor conducted a performance review of the West Virginia Office of Technology pursuant to West Virginia Code §4-10-7. The objective of this audit was to determine the effectiveness of the West Virginia Office of Technology's information technology security framework. The issues of this report are highlighted below.

Frequently Used Acronyms in the Report:

BRIM – Board of Risk and Insurance Management
CIO – Chief Information Officer
CISO – Chief Information Security Officer
CSO – Cyber Security Office
GAO – United States Government Accountability Office
GRC – Governance, Risk and Compliance
NIST – National Institute of Standards and Technology
OT – West Virginia Office of Technology
PERD – Performance Evaluation and Research Division

Report Highlights:

Issue 1: The West Virginia Cybersecurity Office Has Not Fulfilled the Legislative Mandate of Developing a Statewide Cybersecurity Program

- The West Virginia Office of Technology (OT) paid over $1.3 million for two contracts to develop an enterprise cybersecurity program for the State of West Virginia and purchased software for conducting risk assessments, known as a Governance, Risk, and Compliance tool.

- The requirements of the contract were fulfilled within the required two-year period and turned over to OT for statewide implementation in January 2022; however, OT has not rolled out the program to state agencies or used the GRC risk assessment software beyond a pilot program.

- As a result, OT is neither collecting the risk assessments from state agencies, as required by Code, nor is it submitting the cybersecurity status reports to the governor or the Legislature.

PERD's Response to the Agency's Written Response

PERD received the OT's response to the review on September 30, 2025 (see Appendix C). Regarding Recommendation 1, the OT asserts that the agency "always operated an effective statewide cybersecurity program that included risk assessments and reporting." PERD's recommendation would require the OT to collect risk assessments to fully implement the cybersecurity framework as the Code requires and specifies. The OT has not provided PERD with evidence that risk assessments exist or have been collected as detailed in W. Va. Code §5A-6B-4(8), including “an analysis and evaluation of each agency or entity’s cybersecurity readiness, ability to keep user data safe, data classifications, and other steps that the agency or entity has taken towards information technology modernization.” W. Va. Code §5A-6B-6 contains language requiring annual reports submitted to the Joint Committee on Government and Finance and the Governor after December 1, 2019, to include “any recommended statutory changes.” PERD has never been provided with any evidence that the OT ever submitted any annual reports to the Joint Committee on Government and Finance or the Governor.

When the OT responded to PERD’s review, it also provided a report to PERD, as can be seen in Appendix I. Per W. Va. Code §5A-6C-4, this report should have been provided to the Joint Committee on Government and Finance and the report should be electronically transmitted to the members of the committee and be sent to the legislative librarian to be posted on the legislative website. However, PERD has never been provided with evidence OT transmitted an annual report to the legislative librarian or the Joint Committee on Government and Finance. A cybersecurity program that does not adhere in its totality to the Legislature’s directives is not effective and cannot be effective, as it neither contains reporting standards to external and internal entities nor does it address all areas of potential risk.

The OT’s response admits that incidents are occurring. While the OT may have tools to generate reports, the OT’s response further admits the implementation of the cybersecurity program “did not match the documented approach laid-out in statute.” Reporting is only one part of the cybersecurity program but represents one of the key pieces that is missing. The GRC tool also was a critical component of the cybersecurity framework designed to encompass all potential risk areas and would have set the baselines for complete implementation of the cybersecurity framework. The OT may claim that the cybersecurity program is simply a set of necessary tools; however, the tools alone do not replace key components required for a robust cyber security program as directed by Code. Furthermore, the tools alone fail to address all potential areas of risk. Thus, the OT’s statement that they have “always operated an effective statewide cybersecurity program that included risk assessments and reporting” is untrue, regardless of how many tools are being used.

The OT asserts that the cybersecurity program is “robust;” however, if the program does not address all potential areas of risk or operate completely as the Legislature orders – including adequate monitoring and reporting standards between agencies, the OT, the Joint Committee on Government and Finance, and the Governor – then the program cannot be robust. Consequently, PERD did not amend the final statements of the “Issue Summary” within the report as the OT desires, as adherence to every part of W. Va. Code is essential for the cybersecurity program to thrive, and operating a cybersecurity program in a different manner than ordered by the Legislature is tantamount to an agency refusing to use its taxpayer money in a way the governing body has declared to be its intended use.

Regarding Recommendation 2, the OT has stated, “During the pandemic, the CISO at the time determined the specific software was unnecessary and performed functions being provided through other aspects of the cybersecurity program.” This statement does not align with facts, including statements provided by the OT. Figure 1 on page eight of the report shows that the GRC tool was not discontinued until January 1, 2024. Thus, OT continued paying for the software it was not implementing, while West Virginia’s COVID-19 state of emergency terminated on January 1, 2023. Furthermore, the OT has submitted to PERD that plans have been discussed by the OT to advance the cybersecurity program, and that the cybersecurity program became short-staffed, never advancing further. However, the CIO has also informed PERD that the former CISO stated that, due to budget cuts, the GRC tool was no longer needed. Regardless, PERD has never been provided with evidence that the former CISO stated the GRC software was unnecessary because it performed functions that were being provided through other aspects of the cybersecurity program.

Additionally, the OT's response indicates that "existing processes and internal controls sufficiently manage governance, risk, and compliance obligations." However, the GRC tool was intended to encompass all potential risk areas and would set the baselines for full implementation of the cybersecurity framework. If the OT regarded the GRC tool as incapable of fulfilling the desired results, the OT has not provided PERD with documentation showing that the agency identified the GRC tool as not capable of providing those results. Additionally, the OT had the opportunity to address any concerns it had with the Security Risk Solutions and Relational Security Corporation regarding the GRC software or its place within the cybersecurity program. Yet the OT approved the completion of the Cyber Risk Program on January 18, 2022. Either the OT regarded the GRC tool as ineffective and paid for it irrespective of effectiveness, or the OT paid for a Cyber Risk Program utilizing the GRC tool it did not thoroughly assess prior to payment. Regardless, the OT's opinion of the GRC tool as an "unnecessary expense" insinuates that the whole $1.3 million was wasted since the GRC tool was a critical piece of the cybersecurity program. The evidence obtained by PERD indicates the GRC tool could fulfill all the necessary requirements for the cybersecurity program.

Regarding Recommendation 3, the OT states that the "CISO has implemented a plan for receiving annual reports from each agency… These in person [*sic*] meetings are currently underway." The OT has not stated when this plan was implemented. However, PERD's recommendation is not to implement a plan, in-person or otherwise, but to "ensure receipt from each state agency its respective annual report on its cybersecurity readiness, the ability to keep user data safe, and other steps taken towards information technology modernization as required by West Virginia Code §5A-6B-4." These reports are intended to be the output of the GRC tool which identifies all the mandated criteria required by Code. In terms of what the OT says regarding an implemented plan, PERD was not provided any documentation and cannot say if this plan is or is not adequate. However, if the CISO is not receiving these reports, he or she is not aware of an entity's cybersecurity readiness; thus, incapable of accurately assessing an entity's cybersecurity status. This could lead to a gap in the entity's cybersecurity, which neither party is aware of. Furthermore, the documented receipt of the annual reports provides benchmarks for entities' cybersecurity awareness. An in-person meeting is not the same as documenting known vulnerabilities and addressing them systematically and annually. The OT has not given any indication in its response that it intends to ensure receipt of the essential annual reports, contrary to the Legislature's directive in Code.

Regarding Recommendation 4, the OT has attached a report and indicates it has "adopted a plan to submit future annual reports in a timely manner." The OT has provided reports to PERD in response to PERD's recommendation; these reports are included in the agency's response. As seen in Appendix II, the Annual Cybersecurity Status Report shows tools and processes employed by the OT, but it does not show how these tools align with the mandated requirements in Code. "Key Security Operations Metrics" provides values related to the metrics but that provides neither a financial impact nor a security impact, rendering the actual value of the operation unknown. "Legal & Compliance Support Metrics" does not effectively detail types of responses, holds, or support; thereby not providing useful information to the reader. The report does not include any indication that threats exist or addresses needs of the agency. Taken as a whole, the report is vague and promotes the OT's activities without providing concrete information to the reader. Without adequate assessment of real threats to the State's cybersecurity the reader is incapable of determining the complete status of the State's cybersecurity readiness. In the OT's conclusion to the Annual Cybersecurity Status Report, they conclude the agency "delivers a comprehensive and highly effective threat management program, provides endpoint oversight, and supplies continual compliance support." However, the report itself neither addresses how this is being achieved nor is it an accurate picture of the State's cybersecurity readiness by agency or otherwise.

Similar to PERD's fourth response, the OT has submitted to PERD a report found in Appendix I. The report provides no specifics related to the type or incidents reported. The lack of specificity cannot provide adequate information to a reader regarding what the nature of each incident is or where the incidents are occurring. The reporting cannot aid a stakeholder in determining that incidents are occurring and what types are occurring without providing more detail. Furthermore, there is no mention of recommendations made by the Cybersecurity Office on security standards or mitigation that should be adopted per W. Va. Code §5A-6C-4 *et seq*.

Recommendations

1. *The Cybersecurity Office within the West Virginia Office of Technology should begin collecting the risk assessments to fully implement the cybersecurity framework statewide as required by West Virginia Code §5A-6B et seq.*

2. *The Office of Technology should develop and implement a plan of action to re-acquire the Governance, Risk, and Compliance tool that incorporated pilot results.*

3. *The Chief Information Security Officer should ensure receipt from each state agency its respective annual report on its cybersecurity readiness, the ability to keep user data safe, and other steps taken towards information technology modernization as required by West Virginia Code §5A-6B-4.*

4. *The Chief Information Security Officer should annually submit a report to the governor and the Joint Committee on Government and Finance describing the status of the cybersecurity program, including any recommended statutory changes as required by West Virginia Code §5A-6B-6.*

5. *Pursuant to West Virginia Code §5A-6C-4, the Cybersecurity Office should provide electronically on or before December 31st of each year, and when requested by the Legislature, a report to the Joint Committee on Government and Finance that contains the number and nature of cybersecurity incidents reported to it during the preceding calendar year. The report should also be sent to the legislative librarian to be posted on the legislative website.*

ISSUE 1

The West Virginia Cybersecurity Office Has Not Fulfilled the Legislative Mandate of Developing a Statewide Cybersecurity Program

Issue Summary

In 2019, the Legislature created the West Virginia Cybersecurity Office within the Office of Technology (OT). The Cybersecurity Office was created to set cybersecurity standards for all state agencies,[1] and manage a cybersecurity framework that would provide guidance and requirements to state agencies in assessing and improving their ability to prevent, detect, and respond to cyber incidents that threaten agencies' information assets and systems. The Performance Evaluation and Research Division (PERD) found that the Cybersecurity Office spent over $1.3 million for two contractors to develop standards, policies and procedures, and software to assess cybersecurity risks. The contractors developed the required components for a complete cybersecurity program, but the Cybersecurity Office did not roll out the program to state agencies for their adherence, as required by law, to the policies, standards, risk assessments, and reporting requirements. Part of the $1.3 million included the cost of a $189,000 contract for software that would facilitate documenting risk assessments and tracking agencies' status on addressing the risks identified in the risk assessments. The software was renewed for two years for $260,000, but the software was never implemented statewide, and its availability was terminated after the two-year renewal agreement expired. PERD finds that the Cybersecurity Office has not fulfilled the essential mandate of developing a statewide cybersecurity program. The agency is not collecting the required risk assessments, and mandated reports are not being submitted.

The Performance Evaluation and Research Division (PERD) found that the Cybersecurity Office spent over $1.3 million for two contractors to develop standards, policies and procedures, and software to assess cybersecurity risks. The contractors developed the required components for a complete cybersecurity program, but the Cybersecurity Office did not roll out the program to state agencies for their adherence, as required by law, to the policies, standards, risk assessments, and reporting requirements.

The software was renewed for two years for $260,000, but the software was never implemented statewide, and its availability was terminated after the two-year renewal agreement expired.

The Legislature Created the West Virginia Cybersecurity Office in 2019 to Establish a Statewide Cybersecurity Program for Applicable State Agencies

[1] *West Virginia Code §5A-6B-1(b) excludes higher education institutions, the State Police, state constitutional officers identified in West Virginia Code §6-7-2, the Legislature and the Judiciary from the provisions of the Cybersecurity Office. However, these exempt entities or other political subdivisions of the state may enter into agreements with the Cybersecurity Office if they desire to voluntarily participate in the cybersecurity program (W. Va. Code §5A-6B-3(b)(9)).*

In 2019, the Legislature passed House Bill 2452 which created the West Virginia Cybersecurity Office within the Department of Administration's Office of Technology (West Virginia Code §5A-6B-1). The bill charged the Cybersecurity Office with developing a cybersecurity program consisting of standards, policies and procedures, and cyber risk assessments for departments, agencies, and boards within state government to incorporate in their use of information technology infrastructure. The Cybersecurity Office is further charged with managing the cybersecurity framework by assisting and guiding state agencies in developing their cybersecurity plans and procedures. The overarching intention of the cybersecurity framework is defined by W. Va. Code §5A-6B-2, as *"computer technology security guidance for organizations to assess and improve their ability to prevent, detect, and respond to cyber incidents."*

The bill charged the Cybersecurity Office with developing a cybersecurity program consisting of standards, policies and procedures, and cyber risk assessments for departments, agencies, and boards within state government to incorporate in their use of information technology infrastructure.

House Bill 2452 placed the Cybersecurity Office under the supervision and control of the Chief Information Security Officer (CISO), who is responsible for setting the standards and managing the cybersecurity framework. The major responsibilities of the CISO and applicable state agencies are described in Table 1. Once the cybersecurity framework is completed, the CISO would be responsible for having it rolled out to state agencies. State agencies would have the responsibility of adhering to the standards, following the established policies and procedures, and conducting risk assessments with the assistance and guidance of the CISO. If the duties and responsibilities of the CISO and state agencies are carried out as stipulated in statute, then their coordinated efforts would represent a complete cybersecurity program in which the CISO would be assisting state agencies in addressing cyber risks and ensuring that agencies understand their responsibilities for protecting their information systems and data.

Once the cybersecurity framework is completed, the CISO would be responsible for having it rolled out to state agencies.

Table 1
Statutory Responsibilities for Cybersecurity

Powers and Duties of CISO Under W. Va. Code §5A-6B-3	Responsibilities of Agencies for Cybersecurity Under W. Va. Code §5A-6B-4
Develop policies, procedures and standards for an enterprise cybersecurity program.	Undergo appropriate cyber risk assessment as required by the cybersecurity framework or as directed by the CISO.
Create a cyber risk management service to ensure officials manage their agency's cyber risks.	Adhere to the cybersecurity standards established by the CISO.
Establish cyber risk assessment requirements.	Adhere to enterprise cybersecurity polices.
Provide agencies cyber risk guidance.	Complete and submit a cyber risk self-assessment report to the CISO by December 31, 2020.
Assist agencies in developing plans and procedures to recover from a cyber incident.	Manage a plan of action based on the findings of a cyber risk assessment.
Assist agencies in managing the cybersecurity framework.	Submit annual reports to the CISO on the agency's cybersecurity readiness, the ability to keep user data safe, and other steps taken towards information technology modernization.
Ensure uniformity and adequacy of cyber risk assessments.	

Source: West Virginia Code §5A-6B.

The Increasing Risks of Cyberattacks Have Made Broad Cybersecurity Vital

The Legislature's creation of the Cybersecurity Office is consistent with the increasing risk of cyberattacks in the country. In April 2023, the United States Government Accountability Office (GAO) reported in its High-Risk Series that:

> risks to technology systems are increasing. In particular, malicious actors are becoming more willing and capable of carrying out cyberattacks. Such attacks could result in serious harm to human safety, the environment, and the economy. Agencies and critical infrastructure owners and operators must protect the confidentiality, integrity,

The Legislature's creation of the Cybersecurity Office is consistent with the increasing risk of cyberattacks in the country.

> and availability of their systems and effectively respond to cyberattacks.[2]

An effective framework is necessary to achieve the goal of protecting the State's information systems' infrastructure from cyberattacks. The framework OT selected for West Virginia is modeled after the framework developed by the National Institute of Standards and Technology (NIST), which is outlined in the publication "Framework for Improving Critical Infrastructure."[3] The NIST is an independent agency within the U.S. Department of Commerce and its mission is to "*promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."* Cybersecurity is one field that the NIST is well-known for, particularly the NIST framework. It provides comprehensive guidance and best practices that organizations can use to improve cybersecurity through a risk-based approach. It is also one of the most adopted frameworks in both government and the private sector. According to IBM, the NIST framework, *"is flexible enough to integrate with the existing security processes within any organization, in any industry."* Cyber Security Tribe is a peer network of cybersecurity professionals, whose platform is curated by experts in the field of cybersecurity. It reported in its 2025 Annual State of the Industry Report that 68 percent of survey respondents indicated that the NIST framework was the most valuable for guiding their organization's security practices.[4] The NIST framework provided OT with the necessary guidance and approach to setting up the Cybersecurity Office and the cybersecurity program to meet the requirements set forth by the Legislature.

The framework OT selected for West Virginia is modeled after the framework developed by the National Institute of Standards and Technology (NIST), which is outlined in the publication "Framework for Improving Critical Infrastructure".

[2] *United States Government Accountability Office, Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas (High Risk Series), GAO-23-106203, Washington, D.C.: 2023, https://www.gao.gov/products/gao-23-106203.*

[3] *The National Institute of Standards and Technology, United States Department of Commerce, Framework for Improving Critical Infrastructure Cybersecurity, Gaithersburg, MD: April 2018.*

[4] *Cyber Security Tribe, 2025 Annual State of the Industry Report, April 2025, https://www.cybersecuritytribe.com/annual-report. Cyber Security Tribe surveyed 355 cybersecurity practitioners between December 2024 and January 2025. Respondents represented mostly C-Level and VP or Director level staff. Half of the respondents were based in the U.S., 21 percent from Europe and the remaining 16 percent from Latin America, the Asia-Pacific region, the Middle East, and Africa.*

Over $1.3 Million Was Paid to Contractors to Develop a Cybersecurity Program

Rather than developing the cybersecurity program in-house, OT decided to have the work done by private contractors. The OT awarded contracts to two companies totaling $1,344,098. A two-year contract in the amount of $895,098 was awarded to Security Risk Solutions, Inc. on December 2, 2019, to be completed by December 20, 2021. The second contract was awarded to the Relational Security Corporation for risk assessment software beginning on January 1, 2021. The OT renewed the use of the software for an additional two years, from January 1, 2022, through December 31, 2023. The amount of the software contract and renewals totaled $449,000.

The OT awarded contracts to two companies totaling $1,344,098.

The contract with Security Risk Solutions had several major components, with the overall objectives to plan, create, implement and hand over to OT a Cyber Risk Program. The components of the contract are described as follows:

1. **Develop a Cybersecurity Framework:**
    - Define policies for state agencies.
    - Identify the most critical information assets.
    - Evaluate agencies with the highest risk exposure based on their assets and mandated compliance requirements.
    - Align the framework to account for the differing maturity levels of state agencies.
    - Establish a Risk Profiling Procedure and test it on a pilot program of state agencies.

The OT renewed the use of the software for an additional two years, from January 1, 2022, through December 31, 2023.

2. **Develop Cyber Risk Program Documentation:**
    - Create a fully documented Cyber Risk Program.
    - Test the program on a set of pilot agencies, with at least one small and one large agency.
    - Document the approach, tools, and templates for agencies to apply the framework and manage their audit and assessment activities.
    - Incorporate and document lessons learned after the pilot program is executed.
    - Remediate any issues identified.

3. **Assist in Developing a Compliance Audit Solicitation:**
    - Define specifications to be used in a solicitation that state agencies can use to procure a third party to evaluate their adherence to the security standards.

- The solicitation should seek a vendor that will identify and analyze an agency's risk and apply appropriate security controls.

4. **Assist in Developing a Solicitation for Governance, Risk and Compliance (GRC) Software:**
    - Assist OT in developing a solicitation for GRC software that conducts qualitative and quantitative risk assessments, captures audit results, and tracks actions taken in response to risk assessments.
    - Implement the GRC software.
    - Customize the software to align with state-specific requirements.
    - Train users of the GRC software and develop policies and procedures for the use of the software.

5. **Full Implementation:**
    - Based on the results of the previous pilot program, create a roll-out plan to incrementally deploy the cybersecurity framework and Cyber Risk Program to state agencies.
    - Include a communication plan and education.
    - Include a plan to deploy the framework and audit execution across all agencies.

6. **Provide Ongoing Support:**
    - Develop the financial rates model, based on a charge-back model, by which the OT can appropriately charge agencies to cover the projected expenses of the Cyber Risk Program.
    - Ensure that the Cyber Risk Program services are trackable in order that the OT can charge an appropriate fee for the services.
    - Assist OT in establishing pricing for various aspects of the Cyber Risk Program.

The GRC tool, or risk assessment software, developed by the Relational Security Corporation was required to document risk assessments, capture audit results, and track agencies' status on applying the necessary controls to address the identified risks.

The GRC tool, or risk assessment software, developed by the Relational Security Corporation was required to document risk assessments, capture audit results, and track agencies' status on applying the necessary controls to address the identified risks. The Compliance Audit Solicitation was included to allow agencies a means to procure a third party to evaluate their adherence to security standards. The Risk Profiling Procedure was designed to provide a prioritized inventory of the most significant risks identified, identify the necessary controls, and determine whether the controls have been implemented. Once the risk profile was created, Security Risk Solutions would test the profile through a pilot program, and document and remediate any issues identified. The pilot agencies were the West Virginia Tax Division and the Board of Risk and Insurance Management.

The Cyber Risk Program Was Completed and Turned Over to OT, but OT Has Not Rolled Out the Program to State Agencies

The contract with Security Risk Solutions specified eight milestones in which the contractor would be paid upon completion of each milestone and approved by OT. Table 2 shows the invoice amounts paid and the contract titles of the milestones. The GRC software was tested through the two pilot agencies: the West Virginia Tax Division and the Board of Risk and Insurance Management. The findings from the pilot were incorporated into the GRC software and the standards were integrated into the cybersecurity framework by December 30, 2021. Security Risk Solutions created the *West Virginia Risk Assessment User Guide* to provide a step-by-step guide for agencies to complete risk assessments through the GRC software. Security Risk Solutions also provided the rollout plan to guide OT in the execution of the enterprise cybersecurity program.

Security Risk Solutions created the West Virginia Risk Assessment User Guide to provide a step-by-step guide for agencies to complete risk assessments through the GRC software. Security Risk Solutions also provided the rollout plan to guide OT in the execution of the enterprise cybersecurity program.

Table 2
Office of Technology Contracts for the Cyber Risk Program

Security Risk Solutions, Inc.	Amount Paid
Invoice 1 – Developed information security framework	$26,853
Invoice 2 – Reporting templates	$62,657
Invoice 3 – Program roadmap	$134,265
Invoice 4 – Third-party procurement solicitations quantity two (2)	$179,020
Invoice 5 – Implementation of governance tool	$134,265
Invoice 6 – Agency roll-out plan	$89,510
Invoice 7 – Policies and operations procedures	$89,510
Invoice 8 – Assessment results	$179,020
Relational Security Corporation	
GRC Risk Assessment Software	$189,000
2-year Service Renewal Agreement	$260,000
Grand Total	$1,344,098

Source: WVOASIS, calculations are PERD's.

Security Risk Solutions delivered a closeout report on January 5, 2022. The final payment on the Cyber Risk Program contract was approved by OT on January 18, 2022. The documentation obtained and reviewed by PERD indicate that the Cyber Risk Program was completed by Security Risk Solutions and approved by OT, and turned over to OT for implementation across state agencies. Figure 1 shows the major milestones and dates for each milestone in the Cyber Risk Program's development and completion. Despite OT having possession of the completed Cyber Risk Program since January 2022, the program has not been rolled out to state agencies. However, it is unclear why. Those responsible for rolling out the program once it was completed were the CISO and the head of OT, the Chief Information Officer (CIO). The CIO left OT in July 2023 and the CISO left in June 2024. These administrators were still present one to two years after the Cyber Risk Program was completed. Furthermore, the tenures of the new CIO and former CISO overlap by nearly a year, and the new CIO made the decision to cancel the contract on the GRC risk software and informed PERD that the former CISO stated that it was "no longer needed." The timing of the turnover of key OT personnel does not appear to explain why the Cyber Risk Program was not rolled out to state agencies. The current CIO and CISO also confirmed that they were unaware of the cybersecurity program requirements in Code, and they had no knowledge of the completed Cyber Risk Program.

The documentation obtained and reviewed by PERD indicate that the Cyber Risk Program was completed by Security Risk Solutions and approved by OT, and turned over to OT for implementation across state agencies.

Another explanation for not rolling out the Cyber Risk Program is provided in a statement from OT, which is shown below:

> The program was completed on two pilot agencies. During that time, the cyber risk team became short-staffed, and the program never advanced further. The CSO office currently conducts vulnerability management, reviews technology changes, and other services that align with the program.
>
> A plan has been discussed to advance this program from where it left off. This will require hiring new positions. We are currently hiring one position and discussing hiring two more positions to fill deficiencies with our policy development. These positions will transition into helping with this program because their core functions align. The CSO office is also looking at alternative GRC tools that are more affordable.
>
> The GRC tool can also be developed and utilized to assist the CSO Office and the agencies with other audits and

Despite OT having possession of the completed Cyber Risk Program since January 2022, the program has not been rolled out to state agencies. However, it is unclear why.

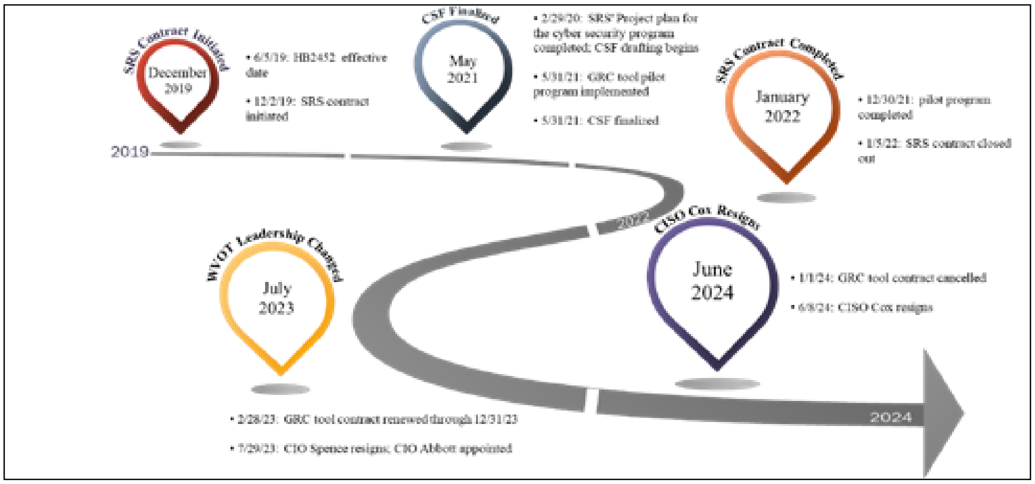
> regulatory compliance issues. We currently do not bill for any of these services and do not have the means to recoup the cost of personnel and the GRC tool. GRC Tools can cost up to a million dollars per year. The GRC solution can also dictate how much time an assessment can take because of the process of entering and tracking all the data. The CSO office will be reaching out to demo these tools to make sure they can function as needed by the CSO office and the agencies.

It is also unclear why OT renewed the GRC Risk Assessment software for two more years if the agency was short of staff at that time.

The abovementioned statement from OT for not rolling out the Cyber Risk Program suggests that a staff shortage and the added cost of the program contributed to not implementing the program. However, the contract with Security Risk Solutions had a component to develop a financial rate model by which the OT could charge agencies appropriate fees for services to cover the projected expenses of the Cyber Risk Program. It is also unclear why OT renewed the GRC Risk Assessment software for two more years if the agency was short of staff at that time. The OT is also indicating that it has developed cybersecurity procedures that align with the Cyber Risk Program, but it is not the Cyber Risk Program itself. The OT has a completed cybersecurity framework that it paid over $1.3 million, and access to a GRC Risk Assessment tool that incorporated test results from a pilot program. The Cyber Risk Program can still be implemented statewide, but the GRC Risk Assessment software is critical to the implementation. Reacquiring the GRC Risk software will be necessary if the Cyber Risk Program is to be implemented.

The Cyber Risk Program can still be implemented statewide, but the GRC Risk Assessment software is critical to the implementation.

Figure 1
Milestones in the Cyber Risk Program Development



- 6/5/19: HB2452 effective date
- 12/2/19: SRS contract initiated

- 2/29/20: SRS' Project plan for the cyber security program completed; CSF drafting begins
- 5/31/21: GRC tool pilot program implemented
- 5/31/21: CSF finalized

- 12/30/21: pilot program completed
- 1/5/22: SRS contract closed out

- 2/28/23: GRC tool contract renewed through 12/31/23
- 7/29/23: CIO Spence resigns; CIO Abbott appointed

- 1/1/24: GRC tool contract cancelled
- 6/8/24: CISO Cox resigns

OT Paid to Renew the GRC Risk Assessment Software for Two Years, but the Software Was Not Used During the Renewal Period

To fulfill the requirement for agency risk assessments, OT purchased the GRC Risk Assessment software from Relational Security Corporation for $189,000. By using the software, agencies would understand their risk environment and use the results to manage their information technology infrastructure from a risk-based approach. The results of the assessment would be integrated into a plan of action to address the findings.

As stated previously, the risk assessment software was tested through a pilot program consisting of the West Virginia Tax Division and the Board of Risk and Insurance Management. According to the final invoice submitted by Security Risk Solutions and approved by OT in January 2022, the findings from the pilot were incorporated into the GRC software. With the pilot project completed in December 2021, OT was in position to roll out the Cyber Risk Program to state agencies following the completion of the pilot. However, no evidence was provided showing that the GRC risk assessment software was used beyond the pilot program. Nevertheless, when the original software contract expired on December 31, 2021, OT renewed it with Relational Security Corporation for two years, January 1, 2022, through December 31, 2023, at a cost of $260,000. Although the software was renewed, there is no evidence that it was used during the two-year renewal period. On January 1, 2024, OT cancelled the contract for the GRC software. OT stated that the contract was discontinued because it was not using the software.

Nevertheless, when the original software contract expired on December 31, 2021, OT renewed it with Relational Security Corporation for two years, January 1, 2022, through December 31, 2023, at a cost of $260,000. Although the software was renewed, there is no evidence that it was used during the two-year renewal period.

Cybersecurity Reports that Are Required by Law Have Not Been Provided by OT or State Agencies

House Bill 2452 included reporting requirements to ensure legislative oversight of the Cybersecurity Office. West Virginia Code §5A-6B-4 required agencies to submit an initial cyber risk self-assessment report to the CISO by December 31, 2020. However, since the cybersecurity framework was not rolled out by OT, state agencies were likely unaware of this requirement. Furthermore, agencies are required to submit annual reports to the CISO by November 1, starting in 2023 and every year after. This annual report is required to contain an analysis and evaluation of an agency's cybersecurity readiness, ability to keep user data safe, data classifications, and other steps that it has taken

West Virginia Code §5A-6B-4 required agencies to submit an initial cyber risk self-assessment report to the CISO by December 31, 2020. However, since the cybersecurity framework was not rolled out by OT, state agencies were likely unaware of this requirement.

towards information technology modernization. There is no evidence that these annual reports have been submitted by state agencies. Also, beginning on December 1, 2019, the CISO is required under W. Va. Code §5A-6B-6 to report annually to the Joint Committee on Government and Finance and the governor the status of the cybersecurity program, including any recommended statutory changes. The annual report is also required to include a summary of each agency's cybersecurity readiness report required by §5A-6B-4. In addition, under W. Va. Code §5A-6C-4(a), beginning in 2021, the Cybersecurity Office is required to provide a report on or before December 31st of each year to the Joint Committee on Government and Finance on the number and nature of incidents reported to it during the preceding calendar year. Furthermore, since 2022, this report is to be transmitted electronically to the members of the committee and be placed on the legislative website. PERD found no evidence that this report has been provided as stipulated by law. These reports listed in West Virginia Code are important in understanding the status of cybersecurity within state government; however, none of the reports have been completed as mandated and the current status of the State's cybersecurity is unknown.

PERD found no evidence that this report has been provided as stipulated by law. These reports listed in West Virginia Code are important in understanding the status of cybersecurity within state government; however, none of the reports have been completed as mandated and the current status of the State's cybersecurity is unknown.

While A Comprehensive Cybersecurity Program Is Essential, BRIM Carries Cyber Liability Insurance to Provide Support When There Is Reasonable Suspicion that a Cyber Incident Occurred

The West Virginia's Board of Risk and Insurance Management (BRIM) has annually procured Cyber Liability Insurance. The insurance policy covers 155 state agencies, including higher education institutions and constitutional offices. The policy covers losses or expenses due to cyberattacks that result in network disruptions, security breaches, privacy breaches, loss of access to computer systems or digital assets, and computer system shutdowns, whether voluntary or involuntary. In the following statement, BRIM informed PERD that:

> In the event of a cyberattack, BRIM has access to forensic consultants through its cyber liability insurance coverage if there is reasonable suspicion or evidence that attackers have compromised protected systems or stolen data.

A cyber liability policy is a crucial part of a comprehensive cybersecurity program, but it is not a replacement for one. It is useful in responding to cyber events when they occur but only if they are identified. According to NIST, cyber insurance is a form of risk transfer, since the liability is shifted from the State to the insurer. However, NIST also states that, *"risk transfer reduces neither the likelihood of harmful events occurring nor the consequences in terms of harm to organizational operations and assets, individuals, other organizations, or the Nation."* In other words, it does nothing to reduce the impact an event could have on the confidence of citizens that the State is protecting their private data, nor does it help to correct or mitigate the issues that created the conditions for the event to occur. Cyber insurance is a tool in the cyber response toolbox and should be part of the State's cybersecurity program.

The OT paid over $1.3 million for an enterprise cybersecurity program for the State of West Virginia.

Conclusion

The OT paid over $1.3 million for an enterprise cybersecurity program for the State of West Virginia. The program was completed and approved by OT within the contracted two-year period and turned over to OT for implementation. Despite the completion of the Cyber Risk Program in January 2022, OT has not rolled out the program to state agencies or used the GRC risk software beyond the pilot program. Moreover, the agency has developed cybersecurity procedures that align with the Cyber Risk Program, but this approach is not a roll out of the Cyber Risk Program that the State paid over $1.3 million. The Legislature mandated the development of a cybersecurity framework in 2019 to guard state agencies against the rising risks of cyberattacks. However, as of 2025, such a program has not been implemented throughout state agencies.

Despite the completion of the Cyber Risk Program in January 2022, OT has not rolled out the program to state agencies or used the GRC risk software beyond the pilot program.

Recommendations

1. *The Cybersecurity Office within the West Virginia Office of Technology should begin collecting the risk assessments to fully implement the cybersecurity framework statewide as required by West Virginia Code §5A-6B et seq.*

2. *The Office of Technology should develop and implement a plan of action to re-acquire the Governance, Risk, and Compliance software that incorporated pilot results.*

3. *The Chief Information Security Officer should ensure receipt from each state agency its respective annual report on its cybersecurity readiness, the ability to keep user data safe, and other steps taken*

towards information technology modernization as required by West Virginia Code §5A-6B-4.

4. *The Chief Information Security Officer should annually submit a report to the governor and the Joint Committee on Government and Finance describing the status of the cybersecurity program, including any recommended statutory changes as required by West Virginia Code §5A-6B-6.*

5. *Pursuant to West Virginia Code §5A-6C-4, the Cybersecurity Office should provide electronically on or before December 31st of each year, and when requested by the Legislature, a report to the Joint Committee on Government and Finance that contains the number and nature of cybersecurity incidents reported to it during the preceding calendar year. The report should also be sent to the legislative librarian to be posted on the legislative website.*

Appendix A
Transmittal Letter

WEST VIRGINIA LEGISLATURE
Performance Evaluation and Research Division

1900 Kanawha Blvd. East
Building 1, Room W-314
Charleston, WV 25305-0610
(304) 347-4890

John Sylvia
Director

July 24, 2025

Heather Abbott, Chief Information Officer
West Virginia Capitol Complex, Building 5, 10th Floor
1900 Kanawha Blvd, E.
Charleston, WV 25305

Dear CIO Abbott:

This is to transmit a draft copy of the Agency Review of the West Virginia Office of Technology. This report is tentatively scheduled to be presented to the Joint Committee on Government Organization during the September 7-9, 2025, interim meetings. We will inform you of the exact time and location once the information becomes available. It is expected that a representative from your agency be present at the meeting to answer any questions committee members may have during or after the meeting.

We need to schedule an exit conference to discuss any concerns you may have with the report. We would like to meet on a day from Wednesday, July 30, 2025, to Tuesday, August 5, 2025. Please contact us to schedule a time. In addition, we will need your written response by noon on Tuesday, August 19, 2025, for it to be included in the final report. If your agency intends to distribute additional material to committee members at the meeting, please contact the House Government Organization staff at 304-340-3192 by Thursday, September 4, 2025, to make arrangements.

We request that your personnel not disclose the report to anyone unaffiliated with your agency. However, the Performance Evaluation and Research Division advises that you inform any non-state government entity of the content of this report if that entity is unfavorably described, and request that it not disclose the content of the report to anyone unaffiliated with its organization. Thank you for your cooperation.

Sincerely,
John Sylvia
John Sylvia

Enclosure

c: Eric Householder, Cabinet Secretary
Department of Administration

Appendix B
Objective, Scope and Methodology

The Performance Evaluation and Research Division (PERD) within the Office of the Legislative Auditor conducted this Agency Review of the West Virginia Office of Technology (OT) as required and authorized by the West Virginia Performance Review Act, West Virginia Code §4-10-7. The purpose of the OT, as established in West Virginia Code §5A-6 *et seq*., is to advise and make recommendations to all state spending units on their information systems and to oversee coordination of the State's technical infrastructure.

Objective

This review's objective was to determine the effectiveness of the West Virginia Office of Technology's information technology security framework.

Scope

The scope of this review covers the effectiveness of the OT's cybersecurity framework based on the extent to which it includes the required elements of the adopted cybersecurity standards and the status of executive branch agencies that have adopted the cybersecurity framework. This was a high-level review of the control environment that focused on the policies, procedures, and associated activities to determine if the framework provided a holistic approach to IT security for the State of West Virginia. While the audit team did not test individual controls, the evaluation considered the presence of oversight controls that ensure activities are carried out as intended. The timeframe of the audit included the previous five and a half fiscal years (2019 through the first half of 2024) to cover the period that the Cyber Security Office (CSO) was created and required to report to the Joint Committee on Government and Finance on the status of the state's cybersecurity readiness.

The CSO is one of several subsections of the Office of Technology. The other sections include administration, communications, IT governance, networking, operations, and records management. These sections were not evaluated in this review because they do not play a critical role in executing part or all of the cybersecurity framework. The agency reports required under W. Va. Code §5A-6B-4 were to be included as part of the assessment to determine the extent to which the framework is being applied by state agencies. During the audit, it was discovered the WVOT has not implemented the cyber security program beyond a pilot program of two agencies. Therefore, required agency reports have not been generated, rendering the audit team unable to review the agency assessments.

Methodology

PERD gathered and analyzed several sources of information and conducted audit procedures to assess the sufficiency and appropriateness of the information used as audit evidence. The information gathered and audit procedures are described below.

PERD staff visited the OT's office in Charleston and met with its executive staff. Testimonial evidence was gathered for this review through interviews with the OT's executive staff to gain a better understanding of the OT's internal controls, policies, and procedures. All testimonial evidence was confirmed by written statements and in some cases by corroborating evidence.

To determine the effectiveness of OT's cybersecurity framework, PERD used the following methodology:

PERD obtained testimonial evidence from OT administration confirming that the cyber security program was not utilizing the cybersecurity framework to manage the cybersecurity program as required by Code. This allowed PERD to determine the effectiveness of the cybersecurity framework at a high level of administration. Testimonial evidence gathered for this review through interviews with OT's staff or other agencies was to gain an understanding of agencies' policies, procedures, or internal controls. Testimonial evidence was confirmed by written statements and in some cases by corroborating evidence.

To gain an understanding of the work done by the contractors in the development of the cybersecurity program and the cybersecurity framework, PERD obtained agency administrative testimony and obtained documentation from OT and the West Virginia Our Advanced Solution with Integrated Systems (WVOASIS), the State's Enterprise Resource Planning system. OT's current executive officers claimed to have little knowledge of the program's development and did not have all the documentation associated with it. The documentation OT did provide included the West Virginia Cybersecurity Framework, handbooks and user guides for the risk assessment software, and other documents related to gather information about the State's IT systems and their controls. Documentation obtained through WVOASIS included the contracts, invoices, and change orders. PERD utilized these documents to determine if the milestones of the contract were achieved and to gain insights as to potential causes for the CSF not being implemented.

The Office of the Legislative Auditor reviews the statewide single audit and the Division of Highways financial audit annually with regards to any issues related to WVOASIS. The Legislative Auditor's staff requests and reviews on a quarterly basis any external or internal audit of WVOASIS. In addition, through its numerous audits, the Office of the Legislative Auditor continuously tests the WVOASIS financial information. Also, at the start of each audit, PERD asks audited agencies if they have encountered any issues of accuracy with WVOASIS data. Based on these actions, along with the audit tests conducted on audited agencies, it is our professional judgement that the information in WVOASIS is reasonably accurate for auditing purposes under the 2018 Government Auditing Standards (Yellowbook). However, in no manner should this statement be construed as a statement that 100 percent of the information in WVOASIS is accurate.

PERD conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix C
Agency Response

STATE OF WEST VIRGINIA
DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY
State Capitol
Charleston, West Virginia 25305

Eric L. Householder
Cabinet Secretary

Heather D. Abbott
Chief Information
Officer

West Virginia Office of Technology
Response to PERD Review

Recommendation 1
The Cybersecurity Office within the West Virginia Office of Technology should begin collecting the risk assessments to fully implement the cybersecurity framework statewide as required by West Virginia Code §5A-6B-1 et seq.

WVOT Response:
In a more thorough and proactive effort to comply, the West Virginia Office of Technology (WVOT) implemented a process for agencies to develop and submit an *Annual Cyber Risk Self-Assessment Report.*

Utilizing an enhanced risk assessment tool, WVOT will assist agencies with completing the assessment. Project managers (PM), intergovernmental relationship managers (IRM) and the security risk team will collaborate with agencies to work through an interactive question-and-answer format. The new procedure combines the current report generating mechanisms with augmented features that enable agencies to create reports in an efficient manner.

Please note that WVOT always operated an effective statewide cybersecurity program that included risk assessments and reporting. WVOT employed tools to generate reports which met and exceeded the intended goals of W. Va. Code. While WVOT acknowledges the implementation did not precisely match the documented approach laid-out in statute, a robust cybersecurity program was in place that protected the state's data, networks, and systems. The approach ensured vulnerabilities were identified, communicated, and managed effectively across all participating agencies in the most efficient manner, using the following elements:

EVMS (Enterprise Vulnerability Management Service)
Purpose: Scans every device within each agency.
Functionality: Identifies required patches, specifies the device, agency ownership, and assigns a risk score.

Status: Fully implemented and in use.

MS-ISAC (Multi-State Information Sharing and Analysis Center)
Purpose: Monitors traffic at the network edge, ingress and egress traffic.
Functionality: Detects communication with known malicious IPs or suspicious behavior. Matches flagged IPs to specific state agencies using SOC.
Implementation: In use.

Firewalls with Security Policies
Purpose: Protect agency networks and enforce least privilege.
Functionality: Tailored rules developed with each agency as new applications and connections are added. Firewalls score the risk of these rules and connections.
Status: Continuously managed and adjusted with agencies.

IRM (Intergovernmental Resource Managers)
Purpose: WVOT Employees serve as relationship managers between OT and agencies.
Functionality: Review vulnerability reports with agencies. Interpret findings and define agency and WVOT responsibilities. Aid agencies in understanding and managing risk.
Status: Active and ongoing.

ITIPS (Information Technology Investment Portfolio System)
Purpose: Internal program developed by WVOT where staff works with individual agencies to evaluate needs and identify use.
Functionality: The program enables WVOT to maintain an application portfolio which identifies the applications in use by agency, recognizes aging software/hardware, highlights investment opportunities, classifies data, aggregates metrics, produces agency-specific dashboards, and supports agency-level planning meetings.
Status: Implemented and in regular use.

CISA (Cybersecurity and Infrastructure Security Agency) Cyber Hygiene Report
Purpose: Assesses, identifies, and reduces cybersecurity risks.
Functionality: Daily scans of public IPs for the Executive branch. Weekly scans scored by risk. Security uses the reports to match risks with IPs and work with agencies to take necessary action.
Status: In place and actively monitored.

CSET (Cybersecurity Evaluation Tool) provided by CISA
Purpose: Assess, identify, and reduce risks.
Functionality: A free, actively monitored tool that is accessible to government agencies. The WV Cybersecurity Framework based on NIST CSF 2.0 is available, along with other risk and security frameworks. Agencies may utilize this tool to assess risks and share results with WVOT.
Status: In place and actively monitored.

As a result, WVOT requests the final sentences of the "Issue Summary" be edited to read:

PERD finds that the Cybersecurity Office has not fulfilled ~~the essential~~ each step outlined in the mandate ~~of~~ for developing a statewide cybersecurity program~~. The~~ because the agency is not collecting the required risk assessments~~,~~ and mandated reports are not being submitted. However, WVOT operated a cybersecurity program that assessed risks and vulnerabilities in a different manner.

Recommendation 2

The Office of Technology should develop and implement a plan of action to reacquire the GRC tool that incorporated pilot results.

WVOT Response:

Reacquiring the GRC tool is an unnecessary expense. Existing processes and internal controls sufficiently manage governance, risk, and compliance obligations

When combined, WVOT's ITIPS and the CSET provide a similar product with comprehensive results. During the COVID pandemic, the CISO at the time determined the specific software was unnecessary and performed functions being provided through other aspects of the cybersecurity program. In place of the GRC, WVOT uses the CSET tool provided by the Federal Government. This tool meets standards laid out in W. Va. Code for providing risk frameworks that track agency results and generate reports. CSET enables agencies to perform risk assessments at a minimal cost to WVOT and agencies.

Recommendation 3

The Chief Information Security Officer should ensure receipt from each state agency their respective annual report on their cybersecurity readiness, their ability to keep user data safe, and other steps taken towards information technology modernization as required by West Virginia Code §5A-6B-4.

WVOT Response:

The CISO implemented a plan for receiving annual reports from each agency. The plan involves a WVOT resource manager meeting with each agency to walk through a comprehensive cybersecurity and risk assessment. These in person meetings are currently underway.

Recommendation 4

The Chief Information Security Officer should annually submit a report to the governor and the Joint Committee on Government and Finance describing the status of the cybersecurity

program, including any recommended statutory changes as required by West Virginia Code §5A-6B-6.

<u>**WVOT Response:**</u>
Report attached. WVOT adopted a plan to submit future annual reports in a timely manner.

WVOT provided a great deal of information to PERD during the review and was awaiting recommendations before finalizing and submitting the most recent report. WVOT will share the report with the Executive Office and Joint Committee.

<u>Recommendation 5</u>
Pursuant to West Virginia Code §5A-6C-4, the Cybersecurity Office should provide electronically on or before December 31st of each year, and when requested by the Legislature, a report to the Joint Committee on Government and Finance that contains the number and nature of cybersecurity incidents reported to it during the preceding calendar year. The report should also be sent to the legislative librarian to be posted on the legislative website.

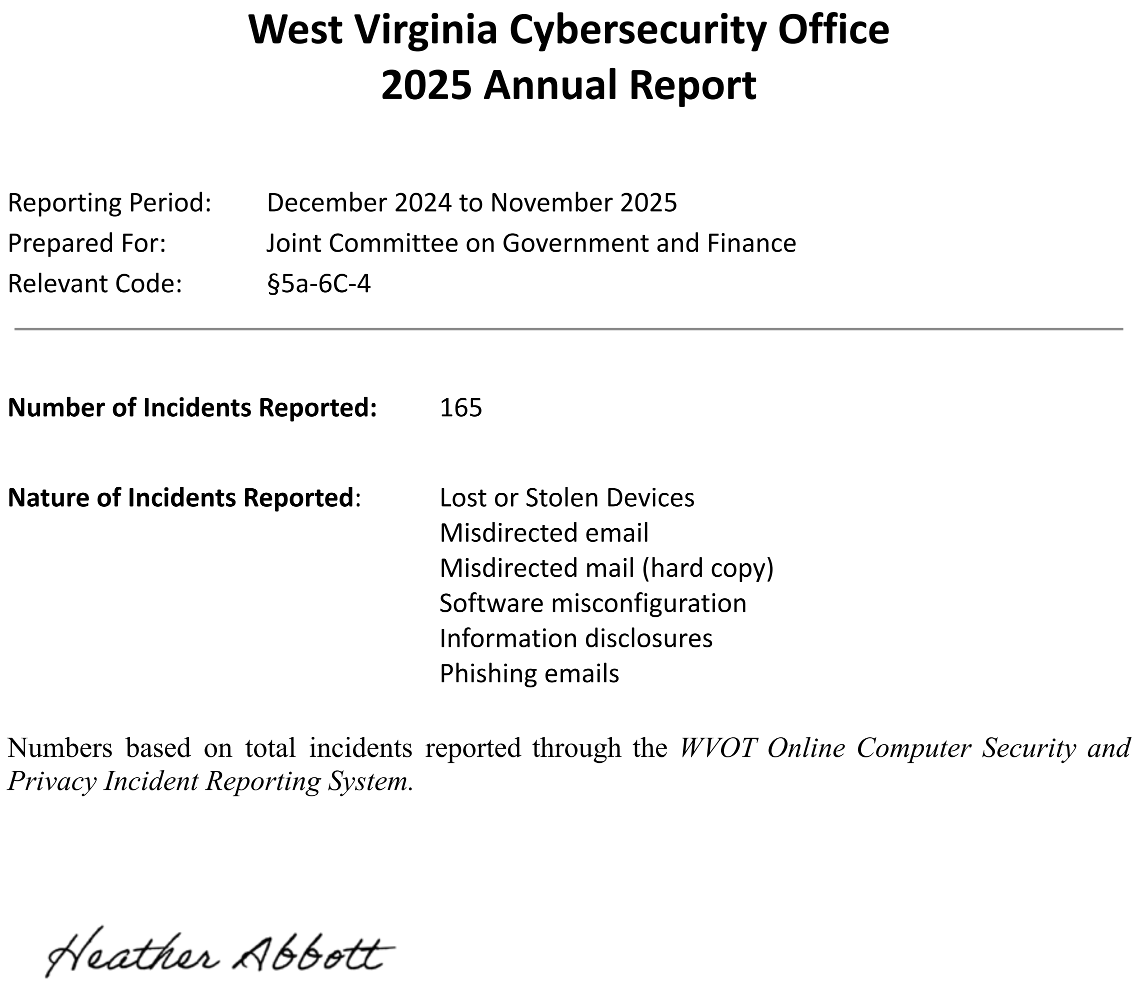
<u>**WVOT Response:**</u>
Report attached. WVOT adopted a procedure to assure reports are submitted annually, moving forward.

WVOT was awaiting PERD recommendations before finalizing and submitting the most recent report. WVOT will share the attached report with the Joint Committee. Furthermore, updates to the *WVOT Online Computer Security and Privacy Incident Reporting System* will enable WVOT to provide more detailed reports in the future.

Heather Abbott

4

Appendix I
West Virginia Cybersecurity Office 2025 Annual Report



West Virginia Cybersecurity Office
2025 Annual Report

Reporting Period: December 2024 to November 2025
Prepared For: Joint Committee on Government and Finance
Relevant Code: §5a-6C-4

Number of Incidents Reported: 165

Nature of Incidents Reported: Lost or Stolen Devices
Misdirected email
Misdirected mail (hard copy)
Software misconfiguration
Information disclosures
Phishing emails

Numbers based on total incidents reported through the *WVOT Online Computer Security and Privacy Incident Reporting System.*

Heather Abbott

Appendix II
West Virginia of Technology Information Security Division Annual Cybersecurity Program Status Report

West Virginia Office of Technology
Information Security Division
Annual Cybersecurity Program Status Report

Reporting Period: December 1, 2024 - November 30, 2025
Prepared For: The Governor and the Joint Committee on Government and Finance

Summary of Agency Cybersecurity Readiness and Modernization

The Office of Technology (WVOT) operates a comprehensive, statewide cybersecurity program designed to protect the state's critical data, networks, and systems from ever-evolving cyber threats. To meet program goals established in West Virginia Code, WVOT employs numerous tools to evaluate agency networks and generate reports which are crucial for maintaining a strong security posture across all state government entities. WVOT leverages up-to-date cybersecurity tools and technologies that enable the office to conduct thorough evaluations of agency networks, identify the most recent vulnerabilities, block threats, and generate detailed reports to support decision-making and guide activity.

Tools and Processes Employed

By integrating these robust tools and processes, WVOT maintains a resilient and secure environment for state agencies that protects critical infrastructure and safeguards data against the ever-evolving landscape of cyber threats:

EVMS (Enterprise Vulnerability Management Service)

Purpose: Scans every device within each agency.
Functionality: Identifies required patches, specifies the device, agency ownership, and assigns a risk score.
Status: Fully implemented and in use.

MS-ISAC (Multi-State Information Sharing and Analysis Center)

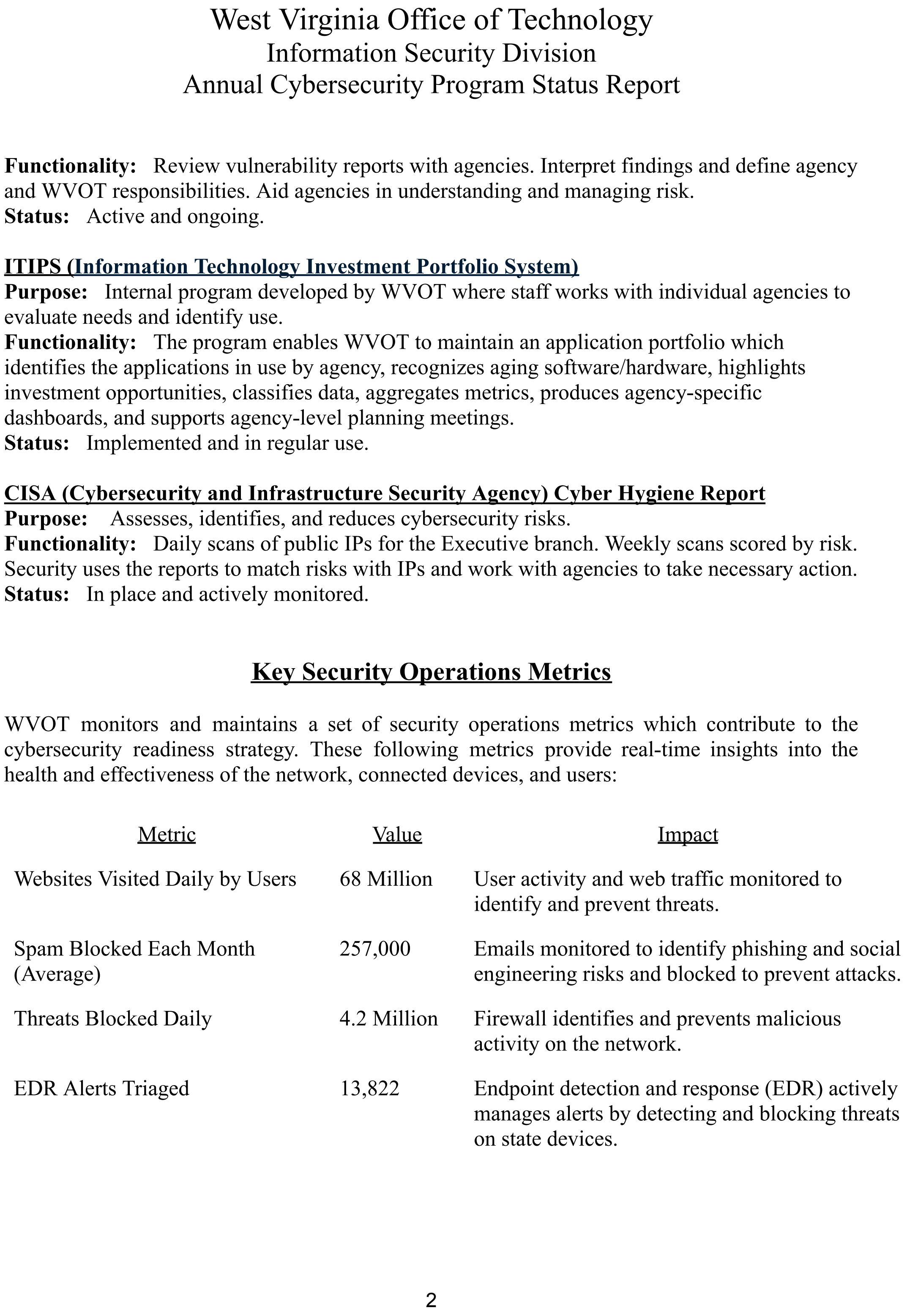
Purpose: Monitors traffic at the network edge, ingress and egress traffic.
Functionality: Detects communication with known malicious IPs or suspicious behavior. Matches flagged IPs to specific state agencies using SOC.
Implementation: In use.

Firewalls with Security Policies

Purpose: Protect agency networks and enforce least privilege.
Functionality: Tailored rules developed with each agency as new applications and connections are added. Firewalls score the risk of these rules and connections.
Status: Continuously managed and adjusted with agencies.

IRM (Intergovernmental Resource Managers)

Purpose: WVOT Employees serve as relationship managers between OT and agencies.



West Virginia Office of Technology
Information Security Division
Annual Cybersecurity Program Status Report

Functionality: Review vulnerability reports with agencies. Interpret findings and define agency and WVOT responsibilities. Aid agencies in understanding and managing risk.
Status: Active and ongoing.

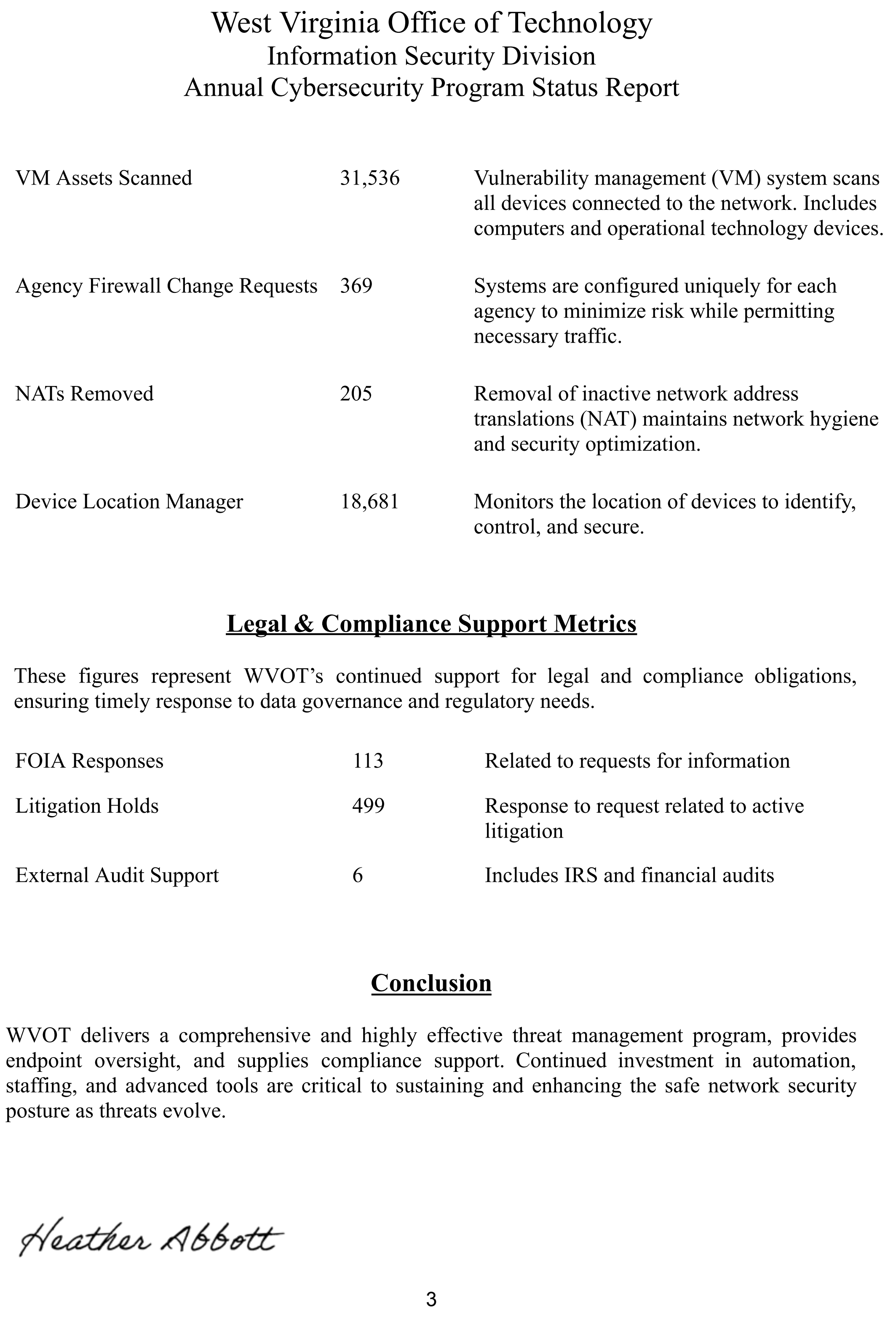
ITIPS (Information Technology Investment Portfolio System)
Purpose: Internal program developed by WVOT where staff works with individual agencies to evaluate needs and identify use.
Functionality: The program enables WVOT to maintain an application portfolio which identifies the applications in use by agency, recognizes aging software/hardware, highlights investment opportunities, classifies data, aggregates metrics, produces agency-specific dashboards, and supports agency-level planning meetings.
Status: Implemented and in regular use.

CISA (Cybersecurity and Infrastructure Security Agency) Cyber Hygiene Report
Purpose: Assesses, identifies, and reduces cybersecurity risks.
Functionality: Daily scans of public IPs for the Executive branch. Weekly scans scored by risk. Security uses the reports to match risks with IPs and work with agencies to take necessary action.
Status: In place and actively monitored.

Key Security Operations Metrics

WVOT monitors and maintains a set of security operations metrics which contribute to the cybersecurity readiness strategy. These following metrics provide real-time insights into the health and effectiveness of the network, connected devices, and users:

Metric	Value	Impact
Websites Visited Daily by Users	68 Million	User activity and web traffic monitored to identify and prevent threats.
Spam Blocked Each Month (Average)	257,000	Emails monitored to identify phishing and social engineering risks and blocked to prevent attacks.
Threats Blocked Daily	4.2 Million	Firewall identifies and prevents malicious activity on the network.
EDR Alerts Triaged	13,822	Endpoint detection and response (EDR) actively manages alerts by detecting and blocking threats on state devices.



West Virginia Office of Technology
Information Security Division
Annual Cybersecurity Program Status Report

VM Assets Scanned	31,536	Vulnerability management (VM) system scans all devices connected to the network. Includes computers and operational technology devices.
Agency Firewall Change Requests	369	Systems are configured uniquely for each agency to minimize risk while permitting necessary traffic.
NATs Removed	205	Removal of inactive network address translations (NAT) maintains network hygiene and security optimization.
Device Location Manager	18,681	Monitors the location of devices to identify, control, and secure.

Legal & Compliance Support Metrics

These figures represent WVOT's continued support for legal and compliance obligations, ensuring timely response to data governance and regulatory needs.

FOIA Responses	113	Related to requests for information
Litigation Holds	499	Response to request related to active litigation
External Audit Support	6	Includes IRS and financial audits

Conclusion

WVOT delivers a comprehensive and highly effective threat management program, provides endpoint oversight, and supplies compliance support. Continued investment in automation, staffing, and advanced tools are critical to sustaining and enhancing the safe network security posture as threats evolve.

Heather Abbott

WEST VIRGINIA OFFICE OF THE LEGISLATIVE AUDITOR

PERFORMANCE EVALUATION & RESEARCH DIVISION

Building 1, Room W-314, State Capitol Complex, Charleston, West Virginia 25305

telephone: 1-304-347-4890 | www.wvlegislature.gov/Joint/perd.cfm | fax: 1- 304-347-4939