Performance Audit Report

Opportunities to Improve Puget Sound Educational Service District No. 121's Information Technology Security

Find out what's new at SAO by scanning this code with your smartphone's camera

Office of the Washington State Auditor
Pat McCarthy

February 2, 2023

Board of Directors
Puget Sound Educational Service District No. 121
Renton, Washington

Report on Opportunities to Improve Information Technology Security

We are issuing this report in order to provide information on the District's information technology security.

Sincerely,

Pat McCarthy, State Auditor

Olympia, WA

TABLE OF CONTENTS

ABOUT THE AUDIT

Critical government services depend on IT systems with confidential information, which must be protected to avoid service disruptions and financial losses

Governments depend on information technology (IT) systems to deliver an array of critical functions. The security of IT systems and related data underpins the stability of government operations, and the safety and well-being of residents. Therefore, protecting these systems is paramount to public confidence, because the public expects governments to protect these systems from IT security incidents that could disrupt government services.

These IT systems also process and store confidential data. Aside from the loss of public confidence, a data breach involving such data can cause governments to face considerable tangible costs. These include identifying and repairing damaged systems as well as and notifying and helping victims of the breach.

> ***IT security incident*** - Any unplanned or suspected event that could pose a threat to the confidentiality, integrity or availability of information assets.
>
> ***Data breach*** – An IT security incident that results in the confirmed disclosure of confidential information to an unauthorized party.

This audit looked for opportunities to improve the District's IT security

To help the Puget Sound Educational Service District No. 121 protects its IT systems and secure the data it needs to operate, we conducted a performance audit designed to identify opportunities to improve IT security. This audit answered the following questions:

- Does the District have vulnerabilities in its IT environment that could lead to increased risk from external or internal threats?
- Do the District's IT security practices align with selected security controls?

Evaluating if there are any problems and vulnerabilities present in the IT environment that could increase risk

To determine if the District has effective IT security practices in place, we conducted tests to determine if selected controls were implemented properly and functioning effectively. We reported the results, including any problems and vulnerabilities we identified, to the District as they were completed.

Comparing the District's IT security program to leading practices

We assessed the District's IT security policies, procedures and practices to selected leading practices in this area to identify any improvements that could make them stronger. We selected leading practices from the Center for Internet Security's Critical Security Controls (CIS Controls),

which were developed by a broad community of private and public sector stakeholders after examining the most common attack patterns. The CIS Controls are a prioritized list of control areas designed to help organizations with limited resources optimize their security defense efforts to achieve the highest return on investment. We gave District management the results of the assessments as they were completed.

Next steps

Our performance audits of local government programs and services are reviewed by the local government's legislative body and/or by other committees of the local government whose members wish to consider findings and recommendations on specific topics. The District's legislative body will hold at least one public hearing to consider the findings of the audit. Please check the District's website for the exact date, time and location. The State Auditor's Office conducts periodic follow-up evaluations to assess the status of recommendations, and may conduct follow-up audits at its discretion. See **Appendix A**, which addresses the I-900 areas covered in the audit. **Appendix B** contains more information about our methodology.

AUDIT RESULTS

We found that, while the District's IT policies and practices partially aligned with industry leading practices, there were areas where it could make improvements. We communicated the detailed results of our work and recommendations to responsible officials and staff for review, response and action. In summary, responsible officials and staff expressed agreement with the audit results and an intent to use them to continue to improve their cybersecurity posture.

Because the public distribution of tests performed, test results, recommendations, and the government's responses could increase the risk to the District, distribution of this information is kept confidential under RCW 42.56.420 (4), and under Generally Accepted Government Auditing Standards, Sections 9.61-9.67.

Recommendations

To help ensure the District protects its IT systems and the information contained in those systems, we make the following recommendations:

- Continue remediating identified gaps.
- Revise the District's IT security policies and procedures to align more closely with leading practices.

Auditor's Remarks

The Washington State Auditor's Office recognizes the District's willingness to volunteer to participate in this audit, demonstrating its dedication to making government work better. It is apparent the District's management and staff want to be accountable to the citizens and good stewards of public resources. Throughout the audit, they fostered a positive and professional working relationship with the State Auditor's Office.

Appendix A: Initiative 900 and Auditing Standards

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to the U.S. Government Accountability Office's *Government Auditing Standards*.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Schedule of Audit Findings and Responses section of this report.

I-900 element	Addressed in the audit
1. Identify cost savings	No. The audit did not identify measurable cost savings. However, strengthening IT security could help the District avoid or mitigate costs associated with a data breach or security incident.
2. Identify services that can be reduced or eliminated	No. The audit objectives did not address services that could be reduced or eliminated.
3. Identify programs or services that can be transferred to the private sector	No. We did not identify programs or services that could be transferred to the private sector.
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	Yes. The audit compares the District's IT security controls against leading practices and makes recommendations to align them.
5. Assess feasibility of pooling information technology systems within the department	No. The audit did not assess the feasibility of pooling information systems; it focused on the District's IT security posture .
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	Yes. The audit evaluates the roles and functions of IT security at the District and makes recommendations to better align them with leading practices.
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	No. The audit did not identify a need for statutory or regulatory change.

I-900 element	Addressed in the audit
8. Analyze departmental performance data, performance measures, and self-assessment systems	Yes. Our audit examined and made recommendations to improve IT security control performance.
9. Identify relevant best practices	Yes. The audit identified and used leading practices published by the Center for Internet Security to assess the District's IT security controls.

Compliance with generally accepted government auditing standards

We conducted this performance audit under the authority of state law (RCW 43.09.470), approved as Initiative 900 by Washington voters in 2005, and in accordance with Generally Accepted Government Auditing Standards (July 2018 revision) by the U.S. Government Accountability Office and *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 B: SCOPE, OBJECTIVES AND METHODOLOGY

Scope

The audit assessed the extent to which the District's IT security programs, including their implementation and documentation, aligned with selected CIS Controls and their supporting sub-controls. This audit did not assess the District's alignment with federal or state special data-handling laws or requirements.

Objectives

To help the District protect its IT systems and secure the data it needs to operate, we conducted a performance audit designed to identify opportunities to improve IT security. This audit answered the following questions:

- Does the local government have vulnerabilities in its IT environment that could lead to increased risk from external or internal threats?
- Do the local government's IT security practices align with selected security controls?

Methodology

To answer the audit objectives, we conducted technical testing on the District's network, and we compared the District's IT security programs to selected leading practices.

Vulnerability Testing

To determine if the District has vulnerabilities in its IT environment we conducted limited technical analysis of select portions of the District's internal network. We performed this work in July 2022 using automated tools configured by our IT security specialists. This included identifying vulnerabilities and assessing them to determine whether they could be exploited.

Internal and external security testing

To determine if the District has vulnerabilities in its IT environment, we conducted internal and external security testing of selected key applications, systems and networks. This work was performed in September and October 2022 by a third-party vendor on our behalf. This work included identifying and assessing vulnerabilities, and determining whether they could be exploited.

Comparing the District's IT security programs to leading practices

To determine whether the District's IT security practices align with leading practices, we interviewed key District IT staff, reviewed the District's IT security policies and procedures, observed District security practices and settings, and conducted limited technical analysis of District systems. This work was completed at the District in October 2022, with some additional follow-up afterwards.

We used selected controls from the CIS Controls, version 8, as our criteria to assess the District's IT security programs and to identify areas that could be made stronger.

CIS is a nonprofit organization focused on safeguarding public and private organizations against cyber threats. The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense and others.

Each control consists of a series of sub-controls that are distinct and measurable tasks. We assessed the District against select sub-controls to determine alignment. We did this by assessing the extent to which the District met each sub-control in two areas:

1. **Implementing** the sub-control
2. **Maintaining documentation** to support the sub-control, such as policies or procedures

Work on Internal Controls

This audit assessed the IT security internal controls at the District. We used a selection of controls from the CIS Controls as the internal control framework for the assessment. Based on an initial assessment, we selected sub-controls from 14 control area to include in the scope. To protect the District's IT systems, and the confidential and sensitive information in those systems, this report does not identify the specific controls assessed during the audit. We completed our assessment for the purpose of identifying opportunities for the District to improve its internal IT security controls, but not to provide assurance on the District's current IT security posture.

INFORMATION ABOUT THE PERFORMANCE AUDIT

Contact information related to this report	
Address:	800 Oakesdale Avenue S.W. Renton, WA 98055
Contact:	Diana Brown, Director Agency Technology
Website:	www.psesd.org

Information current as of report publish date.

Audit history

You can find current and past audit reports for the Puget Sound Educational Service District No. 121 at http://portal.sao.wa.gov/ReportSearch.

ABOUT THE STATE AUDITOR'S OFFICE

The State Auditor's Office is established in the Washington State Constitution and is part of the executive branch of state government. The State Auditor is elected by the people of Washington and serves four-year terms.

We work with state agencies, local governments and the public to achieve our vision of increasing trust in government by helping governments work better and deliver higher value.

In fulfilling our mission to provide citizens with independent and transparent examinations of how state and local governments use public funds, we hold ourselves to those same standards by continually improving our audit quality and operational efficiency, and by developing highly engaged and committed employees.

As an agency, the State Auditor's Office has the independence necessary to objectively perform audits, attestation engagements and investigations. Our work is designed to comply with professional standards as well as to satisfy the requirements of federal, state and local laws. The Office also has an extensive quality control program and undergoes regular external peer review to ensure our work meets the highest possible standards of accuracy, objectivity and clarity.

Our audits look at financial information and compliance with federal, state and local laws for all local governments, including schools, and all state agencies, including institutions of higher education. In addition, we conduct performance audits and cybersecurity audits of state agencies and local governments, as well as state whistleblower, fraud and citizen hotline investigations.

The results of our work are available to everyone through the more than 2,000 reports we publish each year on our website, www.sao.wa.gov. Additionally, we share regular news and other information via an email subscription service and social media channels.

We take our role as partners in accountability seriously. The Office provides training and technical assistance to governments both directly and through partnerships with other governmental support organizations.

Stay connected at sao.wa.gov

- Find your audit team
- Request public records
- Search BARS manuals (GAAP and cash), and find reporting templates
- Learn about our training workshops and on-demand videos
- Discover which governments serve you — enter an address on our map
- Explore public financial data with the Financial Intelligence Tool

Other ways to stay in touch

- Main telephone:
  (564) 999-0950

- Toll-free Citizen Hotline:
  (866) 902-3900

- Email:
  webmaster@sao.wa.gov