BROWN SMITH WALLACE
A MEASURABLE DIFFERENCE
6 CITYPLACE DR. SUITE 900 ST. LOUIS, MO 63141 PH 314.983.1200 FX 314.983.1300 WWW.BSWLLC.COM

Missouri Office of the State Auditor

Cybersecurity Review

April 19, 2018

Missouri Office of the State Auditor
Cybersecurity Review

Table of Contents

INTRODUCTION

Brown Smith Wallace, LLP was requested by the Missouri General Assembly to review the Missouri Office of the State Auditor's (SAO) cybersecurity practices and adequacy of controls for safeguarding sensitive data held by the State Auditor. These non-audit services did not constitute an audit under Government Auditing Standards and such services were not conducted in accordance with Government Auditing Standards. These services were performed using the United States Department of Commerce National Institute for Standards and Technology's (NIST) Cybersecurity Framework published in 2014.

The SAO's Information Technology Team serves a support function, providing executive, administrative, and audit staff with the necessary system tools and training to perform their designated duties effectively. The General Support System for the State Auditor's Office consists of a wide area network with servers located in the Truman Building in Jefferson City and one in each of the three satellite offices in Springfield, Kansas City, and St. Louis. Internet and email capability is provided to the satellite users through the Jefferson City location's connections. Information is transferred between the offices utilizing virtual network connections through the state shared Ethernet/Fiber backbone.

We assessed the adequacy of the policies, procedures, and controls implemented by the SAO to meet the NIST Cybersecurity Framework. Network core services, information security incident response, and security monitoring is the responsibility of the Missouri Office of Administration (OA) and were not included in this assessment. The following table illustrates the IT responsibility division between ~~of~~ the OA and SAO:

Office of the Administration / Information Technology Services Division	State Auditor's Office
• Logical Access for State Applications • Network Management of Core Network Services • Enterprise Change Management • Information Security Incident Response • Security Monitoring • Enterprise Business Continuity and Disaster Recovery Planning	• IT Roles and Responsibilities • IT Governance Within the SAO • Logical Access for SAO Managed Applications • Logical Access for SAO Windows Active Directory • Network Security Within the SAO Network Segment • Security Awareness Training • SAO Application Change Management • Workstation Antivirus and Patching • Data Backups • Continuity of Operations for the SAO • Application Logging

SCOPE

The scope of this assessment addressed the standards of the NIST Cybersecurity Framework. As described in the Introduction section, our review only included cybersecurity practices performed by the SAO. The review did not include practices performed by the Missouri Office of Administration. It included the following:

Function	Category	Subcategory	2018 Status	Observation Reference
Identify	Asset Management (ID.AM)	ID.AM-5; ID.AM-6	**Meets Standard**	
	Business Environment (ID.BE)	ID.BE-1; ID.BE-2; ID.BE-3; ID.BE-4; ID.BE-5	**Meets Standard**	
	Governance (ID.GV)	ID.GV-2; ID.GV-3	**Meets Standard**	
Protect	Access Control (PR.AC)	PR.AC-1; PR.AC-2; PR.AC-3; PR.AC-4; PR.AC-5	**Partially Meets Standards**	**#1**
	Awareness and Training (PR.AT)	PR.AT-1; PR.AT-2; PR.AT-3; PR.AT-4; PR.AT-5	**Meets Standard**	
	Data Security (PR.DS)	PR.DS-1; PR.DS-2; PR.DS-3; PR.DS-4; PR.DS-5; PR.DS-6; PR.DS-7	**Meets Standard**	
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1; PR.IP-2; PR.IP-3; PR.IP-4; PR.IP-5; PR.IP-6; PR.IP-7; PR.IP-8; PR.IP-9; PR.IP-10; PR.IP-11; PR.IP-12	**Partially Meets Standards**	**#1; #2**
	Maintenance (PR.MA)	PR.MA-1; PR.MA-2	**Meets Standard**	
	Protective Technology (PR.PT)	PR.PT-1; PR.PT-2; PR.PT-3; PR.PT-4	**Meets Standard**	
Detect	Anomalies and Events (DE.AE)	DE.AE-1; DE.AE-2; DE.AE-3; DE.AE-4; DE.AE-5	**Meets Standard**	
	Security Continuous Monitoring (DE.CM)	DE.CM-1; DE.CM-2; DE.CM-3; DE.CM-4; DE.CM-5; DE.CM-6; DE.CM-7; DE.CM-8	**Meets Standard**	
	Detection Processes (DE.DP)	DE.DP-1; DE.DP-2; DE.DP-3 DE.DP-4; DE.DP-5	**Meets Standard**	

SCOPE

Function	Category	Subcategory	2018 Status	Observation Reference
Respond	Response Planning (RS.RP)	RS.RP-1	**Meets Standard**	
	Communications (RS.CO)	RS.CO-1; RS.CO-2; RS.CO-3; RS.CO-4; RS.CO-5	**Meets Standard**	
	Analysis (RS.AN)	RS.AN-1; RS.AN-2; RS.AN-3; RS.AN-4	**Meets Standard**	
	Mitigation (RS.MI)	RS.MI-1; RS.MI-2; RS.MI-3	**Meets Standard**	
	Improvements (RS.IM)	RS.IM-1; RS.IM-2	**Meets Standard**	
Recover	Improvements (RC.IM)	RC.IM-2	**Meets Standard**	
	Communications (RC.CO)	RC.CO-1; RC.CO-2; RC.CO-3	**Meets Standard**	

EXECUTIVE SUMMARY

The NIST Cybersecurity Framework is a voluntary set of standards, guidelines and best practices provided to help organizations manage their cybersecurity-related risks. The Framework is a prioritized, flexible, and cost-effective approach that helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

Overall, the SAO has a good understanding of industry best practices and have implemented processes and procedures that satisfy most of the Framework's categories. The recommendations that have been identified are suggestions to improve existing processes and do not represent significant control deficiencies. The two areas that we recommend SAO focus on in the future are as follows:

- Establish Formal Procedures for Tracking Change Requests and Approvals
- Formally Define Information Security and Information Technology Within the Office of the Administration and the Office of the State Auditor

In the section below titled "Observations and Recommendations", we have provided detail on these observations and recommendations.

OBSERVATIONS AND RECOMMENDATIONS

#1 – Establish Formal Procedures for Tracking Change Requests and Approvals

Applicable NIST Cybersecurity Framework Section

PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

PR.IP-3: Configuration change control processes are in place

Observation

The SAO uses Microsoft Team Foundation Server (TFS) to maintain version control for application code changes. We noted that a formal approval mechanism for application code changes is not present. In addition, we found that the SAO's developer has access to the production environment due to the small size of the department. While existing procedures allow the organization to track changes within the code, it does not guarantee those changes will have been formally approved. Without a formalized process to approve changes, unauthorized code may be introduced into the environment. Unauthorized code may negatively affect a system's confidentiality, integrity, and availability.

Recommendations

Procedures should be established to formally track change requests and approvals to assist in ensuring no unauthorized changes are made.

Management Response

The SAO will implement more formal procedures for tracking change requests and approvals regarding application code changes.

#2 – Formally Define Information Security and Information Technology Within the Office of the Administration and the Office of the State Auditor

Applicable NIST Cybersecurity Framework Section
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties

Observation
There are functions identified within the Cybersecurity Framework that fall partially or completely within the responsibility of the Missouri Office of Administration (OA). These include:

- Information Security Incident Response
- Security Monitoring
- Enterprise Disaster Recovery
- Enterprise Changes

Because the OA is responsible for management of core network services, the SAO is reliant on some of the OA's processes for critical system access and other services. Best practice dictates these partnerships should be captured within a formal agreement outlining service expectations and responsibilities of each party involved. The existing SAO Security Plan identifies some responsibilities, but there are no details as to how the entities coordinate their activities or communicate with each other if needed.

In the event of a disaster, unexpected outage, or information security incident, lack of defined responsibilities could lead to essential steps being missed or overlooked. This increases the risk of unauthorized disclosure or loss of data.

Recommendations
A formal agreement should be established with OA which clearly defines the delineation of information security and information technology responsibilities. The agreement should also provide for appropriate coordination and communication for any shared functions.

Management Response
The State Auditor's Office agrees with the audit comments that "[t]here are functions identified within the Cybersecurity Framework that fall partially or completely within the responsibility of the Missouri Office of Administration (OA)." Further, the Office concurs that "the SAO is reliant on some of the OA's processes for critical system access and other services." The State Auditor's Office will pursue discussions of interest and advocate for a formal agreement between the Office of Administration and the State Auditor's Office. However, it is ultimately up to the Office of Administration if a formal agreement can be established.